INFORMATION MANAGEMENT

50TH YEAR

AN ARMA INTERNATIONAL PUBLICATION

MARCH/APRIL 2016

Conducting a **Business and Systems Analysis** to Protect Your ECM Investment Page 20

Benefiting from the NIST Cybersecurity Framework Page 25

What Organizations Must Know About the 'Right to be Forgotten' Page 30

Don't get burned by MISMANAGED INFORMATION.

NEXT LEVEL™ information governance assessment

Your amount of sensitive customer and business data is doubling by the year. And a little loss could have a big impact on your bottom line. Now more than ever, the way you manage your company's information matters. Find out where you stand with the Next Level Information Governance Assessment. Through this self-administered online assessment tool, you'll discover areas of strength. You'll also uncover opportunities for improvement. In the end, you will be empowered to increase your organizational transparency and data integrity.

Start turning information into an asset by visiting **arma.org/nextlevel.**

INFORMATION MANAGEMENT

50TH YEAR

MARCH/APRIL 2016 **VOLUME 50 NUMBER 2**

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Robert Baird, IGP, PMP

Editor in Chief: Vicki Wiler

Contributing Editors: Nikki Swartz, Jeff Whited

Art Director: Brett Dietrich

Advertising Account Manager: Jennifer Millett

Information Management (ISSN 1535-2897) is published bimonthly by ARMA International. Executive, editorial, and advertising offices are located at 11880 College Blvd., Suite 450, Overland Park, KS 66210.

An annual subscription is included as a benefit of professional membership in ARMA International. Nonmember individual and institutional subscriptions are $150/year (plus $20 shipping to destinations outside the United States and Canada).

ARMA International *(www.arma.org)* is a not-for-profit professional association and the authority on governing information as a strategic asset. Established in 1955, the association's approximately 27,000+ members include records and information managers, information governance professionals, archivists, corporate librarians, imaging specialists, legal professionals, IT managers, consultants, and educators, all of whom work in a wide variety of industries, including government, legal, healthcare, financial services, and petroleum, in the United States, Canada, and more than 30 other countries around the globe.

Information Management welcomes editorial submissions. We reserve the right to edit submissions for grammar, length, and clarity. For submission procedures, please see the "Author Guidelines" at *http://content.arma.org/IMM*.

Editorial Inquiries: Contact Vicki Wiler at 913.217.6014 or by e-mail at *editor@armaintl.org*.

Advertising Inquiries: Contact Jennifer Millett at +1 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail *jennifer.millett@armaintl.org*.

Opinions and suggestions of the writers and authors of articles in *Information Management* do not necessarily reflect the opinion or policy of ARMA International. Acceptance of advertising is for the benefit and information of the membership and readers, but it does not constitute official endorsement by ARMA International of the product or service advertised.

Periodical postage paid at Shawnee Mission, KS 66202 and additional mailing office.

Canada Post Corp. Agreement No. 40035771

Postmaster: Send address changes to Information Management, 11880 College Blvd., Suite 450, Overland Park, KS 66210.

It is your life. It is your career. It is your certification.

CRM

In a business world of doing "more with less," your designation as a Certified Records Manager shows that you understand the many facets of the RIM profession.

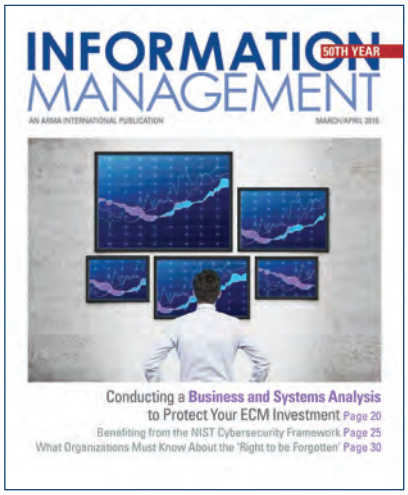
In a business world that is rapidly changing, your designation as a Certified Records Manager shows you are up to date on the latest technology, the latest rules and regulations, and the techniques of the RIM profession.

In a business world in which new jobs are increasingly competitive, your designation as a Certified Records Manager (CRM) demonstrates that you have the experience and expertise to lead change and deploy best practices as they evolve in the RIM profession.

For more information about becoming a Certified Records Manager, contact (518) 694-5362 or visit www.icrm.org

ICRM®
Institute of Certified Records Managers

Common Threads
Throughout the Years



As we celebrate the 50th volume year of this magazine, I am looking back 10, 25, and 50 years at 1967 and 1992 issues of *Records Management Quarterly* (*RMQ*) and 2007 issues of *Information Management Journal* (*IMJ*) to learn more about the foundation and evolution of our flagship publication. It's been interesting and enlightening to see that – as 19th century French novelist Jean-Baptiste Alphonse Karr put it – "The more things change, the more they remain the same" – at least as it concerns topics of interest to our readers.

Just as Mark Grysiuk, CRM, CIP, has written this issue's cover article on conducting a business and systems analysis – in this case for protecting an investment in an enterprise content management system – the April 1967 issue of *RMQ* featured an article on systems analysis for information management by Roger H. Nelson.

Similar to this issue's article from Meg Scofield about using a *de facto* standard, the NIST Cybersecurity Framework, to protect information assets, the April 2007 *IMJ* featured an article about using Australia's *DIRKS Manual* methodology for implementing the first international records management standard, ISO 15489, in an organization.

And, we're still interested in how other countries' standards, laws, and regulations affect our work. Erik Warfel, J.D., IGP, CIPP-US, CISSP, CEDS, writes in this issue about what organizations need to know about the EU's "Right to be Forgotten" mandate; it affects organizations globally.

I am pleased to have *RMQ* and *IMJ* authors still contributing to this magazine. For example, Fred V. Diers, CRM, FAI, writes in this issue about his search to find an effective records and information management or information governance program. His search began well before he wrote "The Bankruptcy of Records Retention Schedules" in the April 1992 *RMQ*.

In that same 1992 issue, there was an article about safe records storage, which our readers are still seeking practical advice about. Robert (Bob) Johnson offers it in his article, "Seven Things Records Destruction Vendors Are Afraid to Tell You."

Flipping through these old magazines, I see many other common threads with today's issues, such as auditing, managing electronic records, and securing information. I also see that despite tremendous industry contraction, many of our present ARMA supporters have been with us throughout much of the past 50 years, including several advertisers in this issue: Fujitsu, NAID, Recall, and OPEX.

If you're interested in seeing association highlights, article names and authors, and advertisers' names and taglines from 50, 25, and 10 years ago, check out "Looking Back" on pages 42-43. This special section is just one of the ways we're celebrating our 50th volume year. Starting with this issue, you can access several pages of "Bonus Content" in the online magazine at *http://imm.arma.org*.

You can let us know what you would like to see in these pages by contacting us at *editor@armaintl.org*.

Vicki Wiler
Editor in Chief

Correction: The print version of the January/February 2016 issue of *Information Management* incorrectly stated the year the American Records Management Association merged with the Association of Records Executives and Administrators to become the Association of Records Managers and Administrators, which we know now as ARMA International. The merger occurred in 1975.

FUJITSU

Get The Most From Your Capture Solution With PaperStream

When it comes to document imaging, the value is in the data. That's why Fujitsu Computer Products of America created a portfolio of software products to complement our industry-leading scanners to help you get the most from your capture solution. At the heart of every high-speed fi Series document scanner is PaperStream IP. The powerful drivers behind PaperStream Capture Pro that ensure high quality image processing—while PaperStream Capture Pro enables efficient document separation and content indexing. For fast, easy-to-use, and simple release, Fujitsu helps you get the most out of data capture by reducing resources, minimizing manual errors, and increasing your bottom line. See us at **www.fcpa.com**

shaping tomorrow with you

PaperStream

PRIVACY

EU, U.S. Agree on New Data Transfer Deal

After three months of intermittent talks, U.S. and European officials have reached a new agreement on how digital data will be transferred from one side of the Atlantic to the other. The Privacy Shield agreement, which still requires political approval, means European data protection authorities will not restrict data transfers as they had planned to if an agreement had not been reached.

According to Reuters, the European Commission said Privacy Shield will place stronger obligations on U.S. companies to protect Europeans' personal data and ensure stronger monitoring and enforcement by U.S. agencies than the previous Safe Harbor agreement.

Since Safe Harbor was invalidated by the European Court of Justice in October 2015, about 4,000 U.S. companies that had relied on it to collect and transfer data out of the EU have been without any legal guidelines for handling information ranging from financial information to social media posts.

"We have for the first time received detailed written assurances from the United States on the safeguards and limitations applicable to U.S. surveillance program," Commission Vice-President Andrus Ansip told the media. "On the commercial side, we have obtained strong oversight by the U.S. Department of Commerce and the Federal Trade Commission of companies' compliance with their obligations to protect EU personal data."

Per the agreement, the United States will create an ombudsman within the State Department to handle complaints and inquiries forwarded by EU data protection agencies, Reuters reported. There will also be an alternative dispute resolution mechanism to resolve grievances, as well as a joint annual review of the agreement.

European data protection authorities said they will also work with the U.S. Federal Trade Commission to police the system.

E-RECORDS

Still Seeking the Paperless Office

Thirty-five years ago, a British-American information scientist introduced the concept of a paperless office. Today, it seems, we are no closer to attaining that scenario, according to a recent survey of UK offices.

Printer company Epson surveyed more than 3,600 European employees, and 83% called the paperless office "unrealistic." It found that hard copies are preferred over digital documents because workers feel the need to share, hand out, and edit reports. In fact, the majority of respondents felt they'd be more likely to make a mistake when editing an electronic document than a paper copy.

According to the survey, 83% of office workers in Europe said a ban on printing would "limit their productivity." Across Europe, office workers spend nearly 19 hours every year walking to and from printers, Epson said, walking more than 110 kilometers (68.35 miles) in the process.

Another survey, from information management firm M-Files, found that 77% of UK businesses still store and manage paper records, with 19% stating they keep all records in paper format and 58% storing data in both paper and digital formats.

PRIVACY

VW Cites Privacy Laws in Refusing to Provide Documents

Volkswagen has refused to provide its executives' e-mails and other communications to U.S. attorneys general who requested the documents as part of their investigations into the company's emissions scandal, according to the *New York Times*.

In September 2015, Volkswagen admitted to installing software to cheat on emissions tests in 11 million diesel vehicles sold worldwide. The *Times* reported that a 48-state civil investigation is being led by several states, including New York and Connecticut, and attorneys general in California and Texas are also looking into the company, which includes the Audi and Porsche brands.

An inquiry by the U.S. Justice Department states that Volkswagen had "impeded and obstructed" regulators and provided "misleading information." Investigators say Volkswagen's actions limit their ability to identify which employees knew about or sanctioned the emissions cheating. Penalties would be greater if the states and others pursuing Volkswagen in court could prove that top executives were aware of or directed the activity.

German investigators said Volkswagen is working with them under the auspices of German law. Klaus Ziehe, a spokesman for prosecutors in Braunschweig, a city close to Volkswagen's headquarters in Wolfsburg, said German law allowed prosecutors to carry out raids of Volkswagen's Wolfsburg offices to gather possible evidence that could include e-mail exchanges, the *Times* reported.

"We can't complain about our cooperation with the company," Ziehe said. "We have the impression that we have received everything that we have specifically requested."

Germany is known for its strict privacy laws, which limit access to data, especially for those outside the European Union. In refusing to turn over evidence to American investigators, Volkswagen has cited the German Federal Data Protection Act, as well as the German Constitution, the European Convention on Human Rights, decisions of the German Constitutional Court and the European Court of Human Rights, "and (for good measure) provisions of the German Criminal Code," according to the *Times*.

INFO SECURITY

Survey: Departing Employees Take Sensitive Data

More than one in four employees take and/or share sensitive company data when leaving a job, according to a recent survey from secure communications solutions provider Biscom.

Technology decision-makers take heed: Survey findings show that the technology a company implements plays a major role in an employee's' decision to take company data. For example, tools like Dropbox, Google Drive, and e-mail make it effortless to take files.

The survey also found:

- 15% of respondents said they are more likely to take company data if they are fired or laid off than if they leave on their own.
- Of those who take company data, 85% report they take material they have created themselves and don't feel doing so is wrong.
- Only 25% of respondents report taking data they did not create.
- About 95% of respondents said that taking data they did not create was possible because their company either did not have policies or technology in place to prevent data stealing or it ignored its policies.

"The survey's results reveal employees as a big security hole," John Lane, CISO of Biscom, said in a statement. "Companies can use this information to understand how they can protect their data. Whether it's updating employee training, establishing stricter company policies to prevent data theft, or obtaining secure tools to store and track company data."

Although stealing data can result in significant security risks, most survey respondents reported that they didn't view it as data theft. Despite the fact that they're taking sensitive information, including company strategy documents, customer lists, and financial data, employees don't consider their actions malicious or even wrong. The report concluded that this may be why data theft is so prevalent.

CYBERSECURITY

Canadian Organization Releases Cybersecurity Guides

A self-regulatory organization that helps monitor Canada's trading industry has released two guides to help investment dealers protect themselves and their clients in the event of a cyber attack.

The Investment Industry Regulatory Organization of Canada (IIROC) introduced "Cybersecurity Best Practices Guide" as a living document that can be updated to include the latest practices on governance and risk management, network security, and more. The 53-page guide also features a cybersecurity incident checklist and a sample vendor assessment, according to *Legaltech News*. The guide covers everything from basic security for computer networks to cost-effective approaches to securing computer systems without the burden of additional regulatory requirements.

The second guide, "Cyber Incident Management Planning Guide," focuses more narrowly on actions to take when a breach occurs. The 29-page document examines the five stages of cybersecurity incident management – plan and prepare, detect and report, assess and decide, respond, and post-incident activity – in addition to the current state of information sharing and breach reporting requirements.

According to the IIROC, the guide provides a framework for developing a plan but is not "intended to function as a working response plan. Rather, each dealer member should develop internal plans as part of their cybersecurity strategy that prepares them in advance for the risks they are most likely to face."

"Active management of cyber risk is critical to the stability of IIROC-regulated firms, the integrity of Canadian capital markets, and the protection of investors," said Andrew Kriegler, IIROC president and CEO, in a statement. "That is why we consulted with the industry, engaged security experts and developed concrete resources to help firms better manage their cyber risks."

The IIROC also noted that it is developing a cybersecurity program to help dealers increase their cybersecurity preparedness. In December, the Canadian government announced plans to launch the Canadian Cyber Threat Exchange in 2016, *Legaltech News* reported. It will be an independent, not-for-profit organization to help businesses protect themselves against attacks through information sharing. Its founding members are Air Canada, Bell Canada, Canadian National Railway Company, HydroOne, Manulife, Royal Bank of Canada, TELUS, TD Bank Group, and TransCanada Corp.

INFO SECURITY

Data Breaches Affect U.S. Consumer Business Decisions

Just how much do U.S. consumers pay attention to data breaches? Enough to consider a company's record before choosing to give it their personal information, a recent survey reveals.

Law firm Morrison & Foerster released "Morrison & Foerster Insights: Consumer Outlook on Privacy," which asked consumers about their attitudes on privacy and data breaches. According to the findings, more than one-in-three U.S. consumers (35%) have made a decision whether to purchase a product from a company because of privacy concerns during the past 12 months. In addition, of those consumers that identified themselves as "concerned" about privacy, 82% said that privacy has adversely affected purchasing a product or service, an increase of 28% from 2011.

However, the survey found that just 22% of consumers have stopped purchasing products or services from a company because of a data breach. But it did find that higher-income and higher-educated consumers are more likely to stop purchasing after a breach.

TICK, TOCK... Every Second Counts

"YOUR SCANNER IS PROBABLY JUST TOO FAST."

There, I said it. Your scanner is either too fast, or you don't have enough preppers. That's why it sits there waiting for work.

How fast a scanner feeds paper doesn't really tell the whole story. If we only looked at the scanner's ability to quickly scan documents, we might surmise that a scanner twice as fast would be twice as beneficial. Makes sense, right? Not so fast! (Pun intended!)

WE KNOW THE DEVIL IS IN THE DETAILS

You've heard it many times, the devil is in the details. And in the case of document scanning…the devil is document prep. Document prep refers to that "necessary process" of making paper documents ready to run through a scanner. Take a look on the old InterWeb at the plethora of instructional videos and PDFs touting the importance of prepping your documents properly. They all detail the steps involved in prepping a banker's box full of folders and archived records of one type or another.

Years ago, we identified over 20 different types of prep activities that may occur while documents are being prepared for scanning. For example: Picture a prepper sitting close to a photocopier, surrounded by rolls and rolls of Scotch tape, with blank 8.5 x 11 sheets of paper and patch sheets in hand.

Thus begins the tedious process of removing staples and paperclips, taping torn documents, photocopying delicate or raggedy pages, securing small or odd shaped pages onto larger ones, unfolding and removing creases from pages, inserting document separators, etc. In addition to these steps, there are a number of other activities dedicated to making the paper easier to feed into a high speed scanner. This time-consuming and monotonous process has been widely accepted as the cost of doing business.

We've heard directly from our customers time and again who verify these industry reports that document prep labor accounts for upwards of 70% of the cost of document scanning.

Heck, even our competitors have had to concede what we've been saying for years: Prep kills profits.

EVERY SECOND COUNTS

So, let's say you are looking at one of those high-priced 6000 DPH (documents per hour) scanners. It doesn't really matter how fast it can scan; it matters how long that scanner operator has to wait for the work to be prepped.

It matters how many hours of front-end labor is required to feed the beast. We have found on average that a great prepper can prep a box of files and documents between 750 and 1000 docs per hour. Some preppers are better, some, well…not so much. Efficient document scanning operations, it should be noted, have squeezed as much time as they can out of the process by eliminating a second here, a couple seconds there. In a box of 2,500 to 3,000 documents, those seconds can really add up, and we applaud the effort.

BUT WHAT IF IT WERE POSSIBLE TO CUT OUT EVEN MORE TIME FROM THE PREP PROCESS?

In March of 2015, OPEX customer, BMI Imaging, installed one Falcon workstation in their Sacramento scanning facility. The results exceeded their expectations. BMI was able to reduce its cost of doc prep labor by 30% per box without sacrificing accuracy or quality. The addition of Falcon led directly to several new projects for BMI's clients who had restricted budgets.

With Falcon, BMI can attack more document scanning jobs than ever before. "We are now able to offer more affordable document scanning services to clients with challenging document preparation work," states Whitney. "Our customers are benefiting from both lower prices and higher quality images."

OPEX PREP-REDUCING SCANNERS

Our scanners provide additional business opportunities and the flexibility to:

- Identify and aggressively bid projects with more challenging paper, or more recurring-revenue transactional work (we have thousands of scanners in the field capturing transactional documents);
- Decrease prep headcount, or increase output using the same number of people; and
- Increase your profit margin.

Now that makes sense.

OPEX CORPORATION

CLOUD

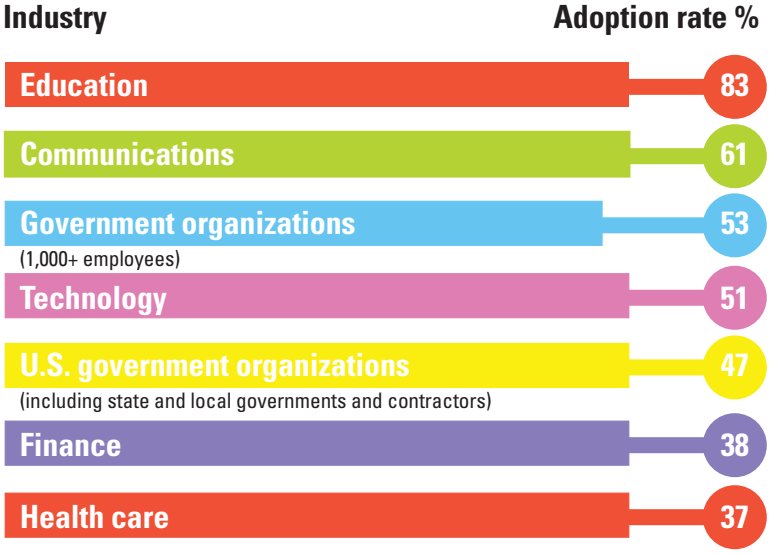
Cloud Adoption Up Across All Industries, Survey Shows

While cloud adoption has significantly increased across all industries, a recent report from data security firm Bitglass revealed that regulated industries are increasingly adopting the cloud. In those industries, adoption jumped from 15% in 2014 to 39% in 2015, with adoption in unregulated industries increasing from 26% in 2014 to 50% last year.

Even heavily regulated industries are increasingly moving to the cloud, the survey shows. Security has always been a concern for these industries; however, the report states that cloud access security brokers (CASB) are filling that gap and enabling widespread adoption of cloud apps across all industries. CASBs offer data-centric security solutions, enabling firms in heavily regulated industries to remain compliant while using public cloud apps, easing the shift away from onsite apps, according to *Legaltech News*.

"Regulated industries have stricter policies in handling sensitive content like personal health information (PHI) and personally identifiable information (PII). Encryption plays a big role in keeping sensitive content from falling into the wrong hands. Traditional cloud solutions do not offer a way to manage and control encryption keys that on-premise solutions offer," Kunal Rupani, principal product manager at Accellion, told *Legaltech News*.

Which industries are racing to the cloud?



Source: Bitglass

Another survey, from Ovum research, revealed that cloud computing adoption is expected to increase over the next decade. A clear majority – 58% – of respondents said they trust the cloud for all business operations. About 78% of survey respondents said they plan to use cloud and software as a service-based applications over the next three years, even for storing and sharing sensitive and regulated data.

Ovum found that data protection is driving cloud adoption because organizations often have limited resources to apply the right data protection to regulated and sensitive data or to prove adequate compliance if the data is stored onsite.

With all that in mind, Ovum says the greatest obstacle facing organizations, lawmakers, and lawyers going forward will be regulating cloud-held data while trying to balance privacy with access and productivity.

Also, the survey found the "most challenging e-discovery environments" may be in South Korea or China, "which have undeveloped or very restrictive climates."

GOVERNMENT RECORDS

NYC Mayor Issues E-Records Directive

Bill de Blasio, New York City's mayor, has issued an executive order to establish standards for proper electronic records management for city agencies through the Department of Records and Information Services (DORIS). The city of 8.4 million residents needs to dispose of 700,000 boxes of documents by 2017.

"This transition will promote improved performance and transparency," the mayor's directive states. "It will be one component of a sensible, comprehensive and compliant information governance program."

'The mayor's directive includes the following guidelines:

- Ensure the preservation of records that have continuing administrative, fiscal, legal, and historical or research value
- Make possible the useful processing of information
- Reduce records storage, equipment, and litigation costs, as well as the costs of other city resources
- Improve operations by documenting agency actions and decisions
- Engage all agency staff in uniform records management practices
- Facilitate access to information in the most efficient manner and at the lowest possible cost
- Ensure agencies operate effectively by appropriately disposing of records that have no archival and minimal value to the city

According to *Politico New York*, the city is currently scanning "millions of papers that are stashed in dusty boxes in private warehouses throughout the city and in New Jersey." The collection totals 2.8 million boxes that will be destroyed.

Half of those are from mayoral agencies, *Politico New York* said, and the other half contains records kept by district attorneys and courts. The DORIS Commissioner's office said it is focusing only on 1.4 million municipal boxes for now. Determining how to digitize the law-and-order papers is a more complicated task. To begin, the city will get rid of boxes containing papers whose required retention periods have expired. There are 169,113 that fall into that category, the agency said.

If the city can get rid of all 700,000 boxes of records by 2017, it estimates it will save $9 million annually in rental costs for records storage.

RIM SERVICES

Iron Mountain/Recall Merger Faces Scrutiny in UK

The Competition and Markets Authority (CMA), the UK's primary competition and consumer authority, said it will investigate Iron Mountain's acquisition of Recall.

Because the companies together provide a large majority of records management and physical offsite data protection services available nationally, the CMA said consumers are worried about loss of competition and choice if the merger goes through. The two companies operate from a total of 59 sites across the UK.

According to the CMA, the merger will be subject to an in-depth phase 2 investigation by an independent group of CMA panel members unless Iron Mountain is able to offer evidence that reduces the competition concerns.

Andrea Coscelli, executive director, markets and mergers, and decision-maker in this case, said:

"Our research and customer responses indicate that these are close competitors in providing 2 distinct types of records and information management services. Iron Mountain is the market leader in both of these markets in the UK. With limited existing competition and no potential new entrants identified, the concern is that the merged company could raise prices or otherwise downgrade those elements of their services which matter to customers."

RIM SERVICES

Microsoft Looks Under the Sea for Future Data Centers

Microsoft researchers believe the future of data centers may lie underwater.

The company said it has tested a prototype of a self-contained data center that can operate hundreds of feet below the surface of the ocean. Because the temperature is chilly down there, the move eliminates an expensive air-conditioning bill, one of the technology industry's biggest obstacles, according to the *New York Times*.

Modern data centers hold thousands of computer servers that create tons of heat. When there is too much heat, the servers will crash. Putting the equipment under cold ocean water could answer the growing energy demands of the computing world because Microsoft is working on placing the system with either a turbine or a tidal energy system to generate electricity, the *Times* said.

The project is code-named "Project Natick," and it might require strands of giant steel tubes linked by fiber optic cables to be placed on the seafloor. Or, Microsoft may suspend jelly bean-shaped server containers beneath the surface to capture the ocean current with turbines that generate electricity, according to the *Times*.

It may sound far-fetched, but researchers believe they could reduce the expense and the deployment time of new data centers from the two years it now requires to just 90 days by mass producing the underwater server containers.

According to the *Times*, the containers could also help speed up web services. Most people now live in urban centers close to oceans but far from data centers, which are usually built in places with lots of space. If servers are placed near users, the delay is reduced.

Microsoft recently conducted a 105-day test of a steel capsule – eight feet in diameter – that was placed 30 feet underwater in the Pacific Ocean off the Central California coast, the *Times* reported. The underwater system, which was controlled from the Microsoft campus in Redmond, Wash., was outfitted with 100 different sensors to measure pressure, humidity, motion, and other conditions in order to learn about operating in an environment where a repairman cannot venture easily or quickly. The new undersea capsules and servers inside are designed to work without needing repairs for as long as five years.

The trial was successful, and the *Times* reported that the research group has started work on an underwater system that will be three times as large. It will be built in collaboration with a developer of an ocean-based alternative-energy system. The developer has not yet been chosen. Microsoft engineers told the *Times* that a new trial will begin next year, possibly near Florida or in Northern Europe, where there are extensive ocean energy projects underway.

According to the *Times*, Microsoft manages more than 100 data centers worldwide, including a more than $15 billion global data center system that now provides more than 200 online services.

CYBERSECURITY

Cyber Attacks on Business Rising

In 2015, 58% of corporate computers had at least one attempted malware attack blocked, up 3% from 2014, according to Kaspersky Lab's Security Bulletin 2015. In addition, file antivirus detection was triggered on 41% of computers or removable media connected to the computers, such as USB sticks or telephones.

E-DISCOVERY

Canada's Information Commissioners Call for a Duty to Document

Canada's information commissioners have asked their respective governments to create a legislated requirement for public entities to document issues related to their deliberations, actions, and decisions.

In a joint resolution, information commissioners expressed concerns about the trend of no records responses for access to information requests. According to the resolution, this weakens Canadians' right of access and the accountability framework that is the foundation of Canada's access to information laws. Without adequate records, it is also difficult for public entities to make evidence-based decisions, fulfill legal obligations, and preserve historical records.

Canada's information commissioners have urged governments to create a positive duty for public servants and officials to create full and accurate records of their business activities. They said this duty must include effective oversight and enforcement that ensure the right of access to public records remains meaningful and effective.

The resolution is available on the websites of the Office of the Information Commissioner of Canada (*www.oic-ci.gc.ca*) and the Office of the Information and Privacy Commissioner for British Columbia (*www.oipc.bc.ca*).

PRIVACY

Survey: New Data Privacy Rules Expected to Cost Companies

A recent Ovum global survey of 366 IT leaders revealed that about 52% of respondents believe the new European Union (EU) General Data Protection Regulation (GDPR) will result in business fines for their company, and two-thirds expect it to force changes in their European business strategy.

Respondents – 63% – also said they think the GDPR regulations will make it harder for U.S. companies to compete, and 70% said the new legislation will favor European-based businesses. Interestingly, respondents cited the United States as the least-trusted country for respecting privacy rights, followed by China and Russia.

More than 70% of respondents expect an increase in spending in order to meet data sovereignty requirements, and more than 30% expect budgets to rise by more than 10% over the next two years as a result of EU regulations. Fines for GDPR violations are potentially 2% of global revenue, which could translate into billions for the world's most profitable companies.

To adapt to the new regulations, 55% of those surveyed said they are planning new training for employees, 51% said they will amend and adapt policies, and 53% said they will prepare by adopting new technologies. Of those who plan to update data privacy strategies in the next three years, 38% plan to hire subject matter experts, and 27% said they will hire a chief privacy officer.

Apparently, such measures are needed: The survey also found that many organizations fall short when it comes to even basic measures to protect data and meet current compliance requirements. For example, just 44% of respondents monitor user activity and use policy-based triggers and alerts. Only 62% have adopted role-based access controls. A little more than 50% actually classify information assets to facilitate controls. Only 54% said they disable PC features, such as external attached drives, while only 57% block access to ungoverned consumer storage and file-sharing apps, such as Dropbox.

The Ovum report recommends organizations conduct a privacy risk assessment, educate their workforces, and ask vendors questions about logical and physical data location as well as service contracts.

INFO SECURITY

Personal Clouds Can Present Security Problems

In an age in which employees can "bring their own cloud" (BYOC) to the workplace, efforts to protect an organization's proprietary information can be challenging.

In a recent action, *PrimePay v. Barnes*, the plaintiff filed a trade secret misappropriation suit against one of its former executives (Barnes) who had established a competing business. The plaintiff sought a preliminary injunction against the operation of Barnes' business, arguing that he had taken confidential company information and stored it in Dropbox.

The plaintiff argued that Barnes used the Dropbox-stored data to help start his new company and then destroyed the materials after the plaintiff warned him "to preserve any PrimePay electronically stored information that he possessed."

The court rejected the plaintiff's argument because Barnes' Dropbox account fell under the company-approved BYOC policy:

"Barnes created the Dropbox [account] … so that he could transfer and access files when he worked remotely on PrimePay matters if he was away from the office, on vacation, or elsewhere and needed access to the PrimePay files, all with the knowledge and approval of [PrimePay owner] Chris Tobin."

Dropbox was a company-approved BYOC provider and, considering factors that suggested Barnes did not access the Dropbox files after leaving his employment with PrimePay, the court found no evidence of trade secret misappropriation and did not issue a preliminary injunction against the operation of Barnes' company. The court did, however, order the destruction of the plaintiff's remaining confidential information that was stored on the Dropbox account.

The decision highlights the importance of developing solid BYOC policies to secure proprietary information and protect other corporate interests. Policies that allow for the use of personal clouds should:

- Clearly describe and define what data can or cannot be transferred to the cloud
- Include audit and enforcement mechanisms to gauge policy observance and disciplinary measures for noncompliance
- Define the nature and extent of the company's right to access, retain, and/or destroy data on a personal cloud for information governance purposes
- Delineate the organization's right to disable a BYOC account either during or after employment
- Outline any employee privacy rights in the data stored in the cloud

GOVERNMENT RECORDS

Ontario: New Fine for Destroying Govt. Records

Anyone caught intentionally altering, concealing, or destroying Ontario government records now will be fined up to $5,000 (Cdn.). Amendments to Freedom of Information and Protection of Privacy legislation at the provincial and municipal levels will require a government organization to develop, document, and preserve its records, according to *The Toronto Sun*.

"Our government takes our record-keeping obligations very seriously we're committed to being open, accountable and transparent," Lauren Souch, a spokesman for Government and Consumer Services Minister David Orazietti, said in an e-mail to the *Sun*. "We promised to open up the government completely, and we have done so to an unprecedented degree."

Organizations that must follow the new rules include government ministries, hospitals, colleges, universities, school boards, municipalities, and police service boards, Souch said.

The penalty comes in response to a concern raised by former Information and Privacy Commissioner Ann Cavoukian that there were no consequences in provincial legislation for the willful destruction of public records, the *Sun* reported. Cavoukian said there had been widespread deletion of e-mails by political staffers as a legislative committee sought records that would have provided more insight into the government's reasons for cancelling gas plants in Mississauga and Oakville at a cost of up to $1.1 billion, according to the *Sun*. Two former senior political aides were charged but have denied wrongdoing.

203 Strong. And Growing.

Congratulations to these **Certified Information Governance Professionals**

Mitchell Abrams
Elizabeth Adkins
Pey-Jia Angell
Christine Ardern
Deborah Armentrout
DeAnna Asscherick
Randy Aust
Christie Baird
Robert Baird
Patty Baldacchino
Salvador Barragan
Christopher Beahn
Richard Berlin
Margaret Boeringer
Isabel Bracamontes
Aaron Bryant
Susan Burd
Kiji Burston
Doug Caddell
Stacie Capshaw
Melissa Carlis
Diane Carlisle
Laurie Carpenter
Alexander Carte
Mark Carter
Peter Casey
Anita Castora
Elizabeth Castro
Tod Chernikoff
Carol Choksy
Vicki Clewes
Andrew Cogan
Julie Colgan
Bud Conner
Dani Cook
Russ Cottle
Marvin Cross
Kristen Crupi
Becky Darsch
Lisa Marie Daulby
Nicholas De Laurentis

Melissa Dederer
G. Derk
Deborah Dotson
Christina Doyle
Sandra Dunkin
Priscilla Emery
Sofia Empel
Tony Epler
Debra Farries
Elizabeth Farthing
Carol Ann Feuerriegel
Glenn Fischer
Matt Fisher
David Fleming
Patricia Franks
Rhonda Galaske
Caroline Gallego
Stephen Garner
Charles Garrett
Irene Gelyk
Sue Gerrity
Kimberly Giertz
Susan Goodman
Joshua Grisi
Komal Gulich
Jocelyn Gunter
Allen Gurney
Michael Haley
Grace Hammar
Joshua Hargrafen
Paula Harris
Matthew Hebert
Charles Herbek
Margaret Hermesmeyer
Caroline Higgins
Gordon Hoke
Patricia Huff
Janice Hulme
Bethany Hynes
Nicolas Inglis
Leigh Isaacs

Mary Janicik
C'Les Jensema
Chris Johnson
Todd Johnson
Deborah Jostes
Deborah Juhnke
Soo Kang
Andrew Keller
James Kennedy
Anju Khurana
Ellie Kim
Michelle Kirk
Monica Kirsch
Tamara Koepsel
Greta Krapac
Peter Kurilecz
Tera Ladner
Richard Lang
Ronald Layel
Anna Lebedeva
Gilles Legare
Donnell Long
Howard Loos
John Loveland
Eric Lynn
Cindy MacBean
Rudolph Mayer
Brian McCauley
Stephanie McCutcheon
Cheryl McKinnon
James Merrifield
Bruce Miller
Sandy Miller
Dana Moore
Dermot Moore
Rafael Moscatel
Linda Muller
Jen Murray
Stephen Murray
Deborah Naas
Joe Nadzam

Lindy Naj
Peggy Neal
Lee Nemchek
Kurt Neumann
Sheri Nystedt
Carolyn Offutt
James Owens
Eleanor Ozaeta
Lewis Palmer
Jadranka Paskvalin
Alan Pelz-Sharpe
Graham Pescod
Denise Pickett
Debra Power
James Presley
Cindy Pryor
Fred Pulzello
Angel Ramos
Tony Ratcliffe
Joshua Rattan
Scott Raynes
Jessica Rickenbach
Deborah Rifenbark
Carol Rittereiser-Coritt
David Rohde
Donna Rose
Shawn Ryan
Kathryn Scanlan
Danna Schacter
Tonia Schneider
Teresa Schoch
Terry Schrader
Karen Schuler
Karen Shaw
Mary Sherwin
William Silvio
David Skweres
Doug Smith
Michael Smith
Natalie Spano
Brian Starck

Jason Stearns
David Steward
Melissa Suek
Lisa Summers
Paula Sutton
Marjorie Swain
Sheila Taylor
Robin Thompson
Kathleen Timothy
Louis Tirado
Brian Tretick
Susan Trombley
Nathan Troup
Brian Tuemmler
Martin Tuip
Amy Van Artsdalen
Paul Van Reed
James Vardon
Katharine Voldal
Jennifer Watters Farley
Bridgett Weldner
Erik Werfel
Steven Whitaker
Kristi Whitmore
Jesse Wilkins
Marc Willemse
Dylan Williams
Steven Williams
Rick Wilson
Terri Wilson
Brett Wise
Jennifer Witt
Kristin Wood
Robin Woolen
Jeffrey Yawman
Cheryl Young
Margo Young
Andrew Ysasi
Ryan Zilm

Application deadlines: March 28, 2016, and November 12, 2016.

Register today at ***www.arma.org/igp.***

GOVERNMENT RECORDS

U.S. FOIA Complaints Rise

U.S. President Barack Obama has been quoted as saying he has led the "most transparent administration in history." But in the past two years, the federal government has received more complaints than ever for not fulfilling public record requests, according to analysis by Syracuse University.

Syracuse found that individuals have filed record numbers of federal lawsuits in 2014-2015 – 64% more than the previous two years – against government agencies for failing to comply with requests made under the Freedom of Information Act (FOIA).

Seven years ago, shortly after taking office, Obama issued a memo stating that the FOIA "should be administered with a clear presumption: In the face of doubt, openness prevails."

Former U.S. Attorney General Eric Holder directed agency and department heads to operate under a presumption of openness.

"I would like to emphasize that responsibility for effective FOIA administration belongs to all of us — it is not merely a task assigned to an agency's FOIA staff," Holder wrote at the time. "We all must do our part to ensure open government."

GOVERNMENT RECORDS

Committee Report: 'FOIA Process Is Broken'

A recent majority staff report from the U.S. House Oversight and Government Reform Committee criticized the current administration and several government agencies for undermining the Freedom of Information Act (FOIA).

"The FOIA process is broken," the report states. "Hundreds of thousands of requests are made each year, and hundreds of thousands of requests are backlogged, marked with inappropriate redactions, or otherwise denied."

According to the report, many agencies are lacking transparency when it comes to the FOIA process by adopting an "unlawful presumption in favor of secrecy" when responding to requests. In some cases, huge sections of information that should have been made public – or were already publicly available – were inappropriately redacted, *FCW.com* reported.

The report cites an investigation by the State Department's inspector general that says the department did not search for e-mail records "as a matter of course." According to the report, "The periodic search for emails was only conducted if a request explicitly referred to 'emails' or 'all records.'"

The 39-page report also says the Justice Department and other federal agencies are contributing to the backlog problem by subjecting requests for politically "problematic or embarrassing" records to an additional layer of review, according to the *Wall Street Journal*.

Some lawmakers criticized the report, blaming GOP budget cuts for the FOIA backlog and noted that previous administrations have not always been transparent.

The report calls for structural reform and new legislation to help move the FOIA process toward greater government transparency.

Lawmakers are trying to strengthen FOIA, which is more than 50 years old. The FOIA Improvement Act of 2015, sponsored by Rep. Darrell Issa (R-Calif.) and Rep. Elijah Cummings (D-Md.), passed the Senate Judiciary Committee in February 2015. Among other things, the bipartisan bill seeks to expand the automatic electronic release of documents that receive multiple FOIA requests and allow for consequences for agencies that miss deadlines, *FCW.com* reported.

According to UPI news, the House of Representatives recently passed the FOIA Oversight and Implementation Act, which calls for creating a single online portal for making FOIA requests. It would limit exemptions that allow federal agencies to withhold information and would require agencies to publicly post frequently requested records online.

In addition, according to UPI, the changes would clarify language allowing agencies to withhold information requested only when there is "foreseeable harm" to an interest protected by a FOIA exemption, such as privacy and national security.

PRIVACY

EU Approves New Data Protection Rules

The Securities and Exchange CoIn December, the European Commission (EC) approved the final version of the General Data Protection Regulation (GDPR). The European Union (EU) Parliament was to authorize it early this year, and it will become law for all 28 member states in 2018.

The new rules usurp the EU's 1995 data protection rules (Directive 95/46/EC). The EC has been working on the GDPR since 2012 to strengthen online privacy rights and boost Europe's digital economy.

Experts say GDPR is the most stringent data privacy regulation yet. The new rules apply extraterritorially and so will impact every entity (data processor or data controller) that holds or uses Europeans' personal data both inside and outside of Europe, according to legal experts.

"GDPR is a paradigm change in the way that data collection and use is regulated. We have moved from an era of relatively laissez-faire regulation of data in Europe to having the most stringent data laws in the world," Ross McKean, partner at law firm Olswang, told *ComputerWeekly.com*.

Key provisions of the GDPR include:

- Instituting more rigorous requirements for obtaining consent for collecting personal data
- Raising the age of consent for collecting an individual's data from 13 to 16 years old
- Memorializing the "right to be forgotten," meaning entities must delete data if it meets the specified criteria
- Requiring entities to notify EU regulators of data breaches within 72 hours of the breach
- Requiring entities that handle large amounts of sensitive data to appoint a data protection officer
- Allowing fines of up to €20 million or 4% of a company's global revenue for non-compliance

According to the *National Law Review*, the most significant change brought about by the GDPR is that jurisdiction is not a physical or geographical barrier because it is now digital, meaning that companies outside the EU will be affected by these new regulations if they collect data that belongs to an EU citizen.

"The GDPR looks to adopt prescriptive rules around how organizations will need to demonstrate that they comply with the GDPR," Vinod Bange, partner and head of the UK data protection/privacy practice at law firm Taylor Wessing, told *ComputerWeekly.com*. "Businesses will have to genuinely adopt governance and accountability standards and not pay lip service to data privacy obligations otherwise they could be in for a surprise as the stiff new fines will apply to that requirement too."

Experts say complying with the new rules will require companies to take steps that include mapping and classifying all personal data; performing risk assessments; designing privacy protections into all new business practices; employing dedicated data protection officers; monitoring and auditing compliance; and documenting everything they do with data and everything done to comply with the GDPR, *ComputerWeekly.com* reported.

Eduardo Ustaran, partner and European head of data protection at law firm Hogan Lovells, told *ComputerWeekly.com* that the GDPR features many requirements to make businesses more accountable for their data practices. "This is the area where the heavy weight of the GDPR will be most felt in practice," he said. "New responsibilities such as data protection by design, data protection by default, recordkeeping obligations, data protection impact assessments, and prior consultation with data protection authorities in high-risk cases will require managerial effort and investment."

In the absence of a new Safe Harbor rule, the GDPR does recognize standard contractual clauses and binding corporate rules as legitimate frameworks for transferring EU citizen data out of the EU.

Key provisions of the GDPR can be found at: *https://edri.org/files/GDPR-key-issues-explained.pdf* and *http://www.twobirds.com/en/practice-areas/privacy-and-data-protection/eu-framework-revision*.

E-DISCOVERY

IRS Erased Hard Drive, Spurning Court Order

Despite a court order, the U.S. Internal Revenue Service (IRS) erased a hard drive belonging to a former top official involved in the agency's much-criticized hiring of law firm Quinn Emanuel Urquhart & Sullivan LLP.

Although a litigation hold had been placed on all materials related to the IRS hiring of the outside firm, the hard drive was erased anyway. The order came in response to a Freedom of Information Act (FOIA) request submitted by Microsoft on the IRS contract with Quinn Emanuel.

According to *Law360*'s report, the IRS informed the U.S. Department of Justice (DOJ) in December that it wiped the hard drive in April 2015, after the hold was in place, according to a filing by the DOJ in a Washington federal court. The hard drive belonged to Samuel Maruca, former director of transfer pricing operations at the IRS Large Business and International Division, who helped hire the law firm.

Quinn Emanuel was apparently hired to pursue Microsoft. Even though it had no prior experience handling sensitive tax data, the outside firm was hired at more than $1,000 an hour, according to court records. The initial contract for work was $2.2 million, *Law360* found.

The hiring decision prompted a probe by Finance Committee Chairman Orrin Hatch (R-Utah), who wrote a letter to the IRS stating that hiring outside contractors was expensive and unnecessary, as the agency already employs about 40,000 people responsible for enforcing tax laws. A federal judge has called the decision "troubling."

It's not the first instance of the IRS failing to preserve critical information. The agency also "accidentally" erased the hard drive belonging to Lois Lerner during investigations into the targeting of conservative organizations. As many as 24,000 e-mails were lost when 422 backup tapes were wiped clean despite an agency-wide preservation order and congressional subpoena. In that case, a report by the House Oversight Committee found that the IRS failed to take simple steps to ensure compliance with the order.

COURT CASE

Agencies Must Manage E-mails by End of Year

By Dec. 16, 2016, all federal agencies are required by the Obama administration's information management policy to manage all government e-mail that qualifies as permanent or temporary records in electronic format.

That means agencies must have in place a method of retaining e-mail records in an electronic system that allows for managing and retrieving records and supports litigation needs, open-government requests, and other archival purposes, according to *FCW*.

According to a report released in December 2015 by the National Archives and Records Administration (NARA), 93% of records managers who reported said they are on track to meet the deadline. NARA said it received 84 reports, for a compliance rate of 94%.

"At this point, we're not aware of any agencies that definitively will not make it," Laurence Brewer, NARA's acting chief records officer, told *FCW*. "The 2016 target is an important one. We do expect all agencies to meet that target. But we do realize that it may not be realistic for 100% of agencies given the complexities of their email systems [and] funding priorities, and of course, now we have a presidential transition that's looming."

Brewer said nearly 80% of agencies "report that they have policies and procedures to manage their email." A majority told NARA they plan to implement the agency's Capstone approach to e-mail management, which identifies accounts of key senior officials and key job functions for automatic preservation, *FCW* reported.

The approach is designed to take some of the guesswork out of e-mail management and nudge agencies toward greater levels of automation. Another goal is to eliminate old-fashioned practices such as manually dragging selected e-mails into folders for preservation.

FCW reported that NARA officials plan to release more detailed criteria soon to tell agencies specifically what they need to do to meet the target. In the meantime, NARA is trying to meet its own targets. A 2014 update to federal records laws gave the agency new oversight and inspection authority. To that end, the Office of the Chief Records Officer has grown and reorganized, and NARA has hired more employees with the technical knowledge to help agency records officers manage e-mail systems. **END**

NEXT LEVEL™
information governance assessment

Your business data is doubling by the year. And all this new data can either help you or hurt you. Find out what it's doing for your company with the Next Level Information Governance Assessment. You'll discover areas of strength and opportunities for improvement. In the end, you will be empowered to increase organizational transparency and data integrity while decreasing risk.

Start turning information into an asset by visiting **arma.org/nextlevel**.

Conducting a **Business and Systems Analysis** to Protect Your ECM Investment

Cleaning, organizing, and classifying content in accordance with information governance policies prior to migrating files to an enterprise content management system are essential to ensuring its successful implementation and adoption and to minimizing operational risks and liability.

Mark Grysiuk, CRM, CIP

To get the best "bang for their buck" from an enterprise content management (ECM) investment, organizations must have or be implementing a formal information governance (IG) program. It also requires them to incorporate a thorough business and systems analysis into the project plan, considering the scope of the technology for the deployment and any third-party applications that may be integrated in subsequent project phases. Just as important, they must invest the necessary time for training and awareness early to avoid a catastrophe later.

If the deployment includes migrating documents from network drives, local drives, and cloud-based e-mail providers, organizations must define the scope of the exercise and assign a reasonable amount of time to the tasks required prior to any migration efforts, including:

- Preparing stakeholders for network drive migrations
- Analyzing business processes
- Assessing recordkeeping requirements
- Preparing for document and e-mail migrations
- Building a sustainable security management framework
- Preparing to go live

Some of these activities may be conducted concurrently, using more than one information management specialist, records analyst, and business analyst.

Preparing Stakeholders

Setting expectations with stakeholders well in advance of the data migration is too important to overlook. Communicate early and often. Let them know a designated analyst may be stopping by to observe how users interact with applications and tools, including e-mail. Remind users that as part of the change management initiative, the IG team must thoroughly understand business requirements.

Keep users apprised of all activities and policy updates that affect them – including those who are on leave – so they will not be surprised by the transition that has taken place when they return. The more transparent the process, the greater the audience captured over the deployment life cycle will be.

Build strong relationships with the IG stakeholders in the business units. For example, work with human resources and others to ensure that the IG stakeholders' job descriptions and salaries are adjusted to reflect the expertise and the level of responsibility they must have to govern the organization's information as the valuable asset it is. Customize training to ensure that it fits each department's unique business processes.

Analyzing Business Processes

Be certain the project team thoroughly understands how stakeholders interact with information. Pay special atten-

Migration Planning Checklist

Use this checklist to help ensure a successful file migration to an electronic content management system.

Communication Planning

- Have all stakeholders been identified – including those on leave?
- Is there a communication schedule?
- Have distribution channels been approved?
- Does the project plan include lunch-and-learn workshops that are customized to specific audiences' requirements?
- Have all stakeholders been trained?

Business and Systems Analysis

- Who accesses this information?
- Have software/hardware requirements been defined (e.g., third-party applications)?
- Are there automated processes storing output in network file server folders? If so, will these processes push these files to the ECM system? If so, has this process been tested?
- Do folder structures contain several thousand folders and files?

Document and E-Mail Management

- Will existing network drive structures be maintained?
- Have out-of-scope formats been identified and scheduled for disposition?
- Do processes involve the development and/or management of audio, video, and imaging?
- Do large formula- and link-driven spreadsheets exist?
- Are users interacting daily with dozens or even hundreds of documents?
- What e-mail messages do users receive that pertain to their responsibilities?
- Are cloud-based e-mail systems used or being considered as part of the migration plan?

Security Management System

- Is there a desire to manage security at the file level?
- To what network drives do users have access?
- Is there a desire to restrict access without valid business reasons?
- Does training material describe how users can best engage support?
- If permissions at the file level are required, does the information owner maintain a listing of those files and their locations?
- Are administrative controls set so users are unable to alter company-approved configuration settings?

tion to who owns information, where the source electronic records reside, security classifications, and vital record status. Include electronic form submission processes that notify stakeholders via e-mail alerts and the metadata associated with those forms. Ask about reports delivered electronically to designated network drive folder structures.

When observing stakeholders' computing habits, address these questions:

- Will users require mapped network drives? If so, it will require additional time for IT to visit workstations to install third-party applications and do the mapping. This activity should not be left to end users, who might misconfigure settings and prevent some ECM functionality from working.
- Do users work with large files? If a lot of large files are being moved at the same time, the spike in traffic can dramatically slow the system and frustrate end users.
- Do file and folder names use special characters, such as #, %, &, and *? Some ECM solutions do not allow special characters, so they must be replaced.
- Do users regularly interact with documents and folder structures containing thousands of files and folders? Because documents on a network drive are often linked to other documents on the drive, there's the risk of breaking those links when migrating to an ECM system. These *living* documents – those that are updated regularly – can within a very short period acquire thousands of versions in an ECM system. Therefore, the organization must define the requirements for retaining versions for operational documents.

If e-mail migrations are in scope, identify stakeholders who are active filers and those who are not, as a different communications strategy will be required for the latter.

Assessing Recordkeeping Requirements

Resist any "just in case" business requirements. Point stakeholders to the records series that align with their departmental objectives. If stakeholders are storing transitory business information, determine the need for this to continue. If it does, a secondary retention code with a shorter retention period may be needed in the ECM system to dispose of those files earlier than the official versions. A more desirable practice is to create an appropriate security group owned by the other business units so external departmental stakeholders can access one version of the truth. (See "Building a Sustainable Security Management System" on page 23.)

Preparing for Document and E-Mail Migrations

ARMA International has published several resources for managing electronic records, including *Developing Electronic File Structures* (ARMA International TR 23-2013). Other standards that may be consulted are ISO-15489:2001 *Information and documentation – Records management – Part 1: General* (which is scheduled to be superseded in 2016) and ISO 16175-2:2011: *Information and documentation – Principles and functional requirements for records in electronic office environments – Part 2: Guidelines and functional requirements for digital records management systems*. (All of these publications are available for purchase at *www.arma.org/bookstore*.)

If budgets permit it, engage a file analysis vendor...

Analyzing Network Drives

Analyzing large, unstructured file repositories of *dark data* – which Gartner defines as "the information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes…" – can be a time-consuming activity.

If budgets permit it, engage a file analysis vendor. File analysis tools can provide quick insight into large repositories by examining creation and modification dates, as well as owner and content types. Other useful functionality includes, but is not limited to, applying security classification to large directory structures and analyzing security groups.

If engaging a file analysis vendor isn't an option, work with IT to identify appropriate file analysis utilities available for free online that can provide some of the same systems-related information. When in doubt, engage a technical expert for assistance.

In partnership with stakeholders, decide whether existing folder structures will be maintained or modified to accommodate IG policies.

Full access to the entire structure is required to understand the existing security framework. Request a listing of all security groups and members, and confirm with the administrator how far down the folder hierarchy rights have been assigned. Expect to see several nested structures with branches extending in many directions, which is common for network drives that have been around for a while.

Deeply nested structures (e.g., mapped three or more levels down from the root folder) can be challenging to configure. Ideally, IT can make recommendations for an ECM structure that resembles the network drive structure users are familiar with already.

If a decision is made to migrate everything within a specific time-frame – the last seven years, for example – get approval to purge all files older than seven years (as well as files with all out-of-scope file formats) before the migration. Qualified ECM implementation developers can map the last modified dates for active network drive files or *sent* and *received* dates for source e-mail applications to the record series status dates in the new system. Disposition reports can be run at a pre-defined date on a regular basis.

Analyzing E-Mail

Think strategically. E-mail is a smoking gun. Conduct as much cleanup as possible prior to any migration from one system to another, including cloud-based e-mail management systems.

Use a risk-based approach to identify stakeholders whose e-mail accounts are more likely to contain business records required for long-term preservation.

Also, consider the following:

- Migrating a single e-mail account could take several hours or longer depending on factors that include volume of e-mail and the source systems. Additional fees may be required if the maximum transfer rate threshold on some third-party cloud-based application programming interfaces have been reached.
- Viewer applications may be required. Depending on the native e-mail application, additional licensing costs might be associated with this requirement.
- An e-mail account containing 50,000 e-mails may double or triple the number of documents in the ECM system if the destination system has been configured to store attachments separately from the e-mail message. E-mail files stored in their native format will keep space requirements at a minimum.
- Allot an appropriate amount of time to these tasks, and set expectations with all relevant stakeholders.

For more information on e-mail management best practices, visit ARMA International's bookstore for a variety of resources, including *E-Mail Retention and Archiving* by William Saffady and *Best Practices for Managing Electronic Messages* (ARMA International TR 24-2013).

Building a Sustainable Security Management System

Thou shalt always comply with security management best practices. Keep it simple. Use access control groups to manage large document repositories. Full rights should be granted only to designated data administrators. Avoid assigning permissions using individual user profiles, and even more so, avoid assigning permissions at the file level.

While there may be exceptions to these rules, they should be few. An organization with thousands of employees requiring individualized permissions at the file level will create an administrative nightmare. Left uncorrected, there will be a lapse in policy adherence. Be sure a process is in place for revoking access as requirements change.

Configure permissions prior to the migration. Post-migration, assigning access rights down a structure containing several thousand files could be a resource-consuming endeavor for some ECM systems. That's because ECM rules for some systems are applied to each object (e.g., files, folders, task lists) one at a time. Depending on web server traffic, it could take several minutes or even hours. Multiply this number by several hundred employees with similar access requirements and a system administrator will be busy doing nothing but adding and revoking permissions on top of the other responsibilities.

Always protect personally identifiable information and other confidential information based on need-to-know principles. Build file plans that factor in these requirements.

Be very careful to avoid creating barriers for users who require access but can't get it because the system is overly protected. When push comes to shove, users will always find a way to circumvent a policy if it disrupts the business process. It's easy for Alice to say that Bob's department cannot be trusted because of a recent incident involving inappropriate exposure. Rather than locking the other group out, a more appropriate solution may be to provide mandatory ethics and security management training for Bob's team more than once per year.

Conduct as much cleanup as possible prior to any migration...

Preparing to Go Live

Many organizations stack or layer applications, such as web distributed authoring and versioning (also referred to as WebDAV) client software and Windows Explorer, on top of their ECM installations to promote user-friendly work environments. If the applications are configured correctly and used appropriately, employees can work in an environment that resembles a network drive without much change to how they do their work. Accessing content is easy. Minimal training is required. Compliance objectives are achieved.

When applications are layered, the number of server requests has a tendency to grow at the bottom of the stack. Add in the complexity of various client software packages, such as Microsoft Office or Adobe Creative Suite, and the quantity of requests can grow.

Without the proper infrastructure in place, a small group of power users accessing and/or moving content frequently from the same workspace can be a strain on systems' operations. (See "Database Blocking" in *More Resources*).

To reduce operational risks, ECM project managers must ensure enough time is set aside for testing layered deployments to determine:

- If there is an increase in requests to the database server in comparison to accessing content directly in the ECM application
- Whether Microsoft Office's Temp File Management will be an issue for preserving versions
- Whether audit history and other mandatory ECM metadata requirements are impacted
- If locked files are intuitive for other users (i.e., is there a prompt advising that the file is locked and can be

viewed only as read only?)
- If custom software coding aligns with best practices and coding standards

Finally, develop training and/or best practices documentation that conforms to the approved deployment. Review these documents regularly or whenever applications are added to the ECM installation. Always remember the need to understand business processes, the uniqueness of added application layers, and the vulnerabilities that may be created if systems aren't tested against approved standards.

Getting it Right

Cleaning, organizing, and classifying content in accordance with IG policies prior to a migration to a new system can be cumbersome tasks. They are, however, necessary tasks. Without them, the result may be, for example:

- A poorly implemented communications strategy that impedes adoption rates
- An undefined and haphazardly deployed security framework that creates a liability risk
- Operational risks associated with noncompliance to information management best practices that will impact the availability and integrity of important business records
- Liability risks if users decide to circumvent policies to prevent disruptions to their business processes

Get it right or pay the price. **END**

Mark Grysiuk, CRM, CIP, *can be contacted at* mgrysiuk@gmail.com.
See his bio on page 47.

Read More About It:

BeyondRecognition. "Email Remediation Step 1: Faceted Deduplication." *http://beyondrecognition.net/email-remediation-step-1-faceted-deduplication*

Broadcast Software International. "Why Nested Folders Should Be Avoided." *www.bsiusa.com/support/FAQ/nested/nested.php*

Download.com. "File List Generator" Download. *download.cnet.com/File-List-Generator/3000-2248_4-10921000.html*

Exterro. "File Analysis Software" Demo. *www.exterro.com/information-governance-software/file-analysis-software/*

Gartner. "Market Guide for File Analysis Software." *www.gartner.com/doc/2853417/market-guide-file-analysis-software*

Gizmo's freeware. "Use the Command Line to Easily Create a List of Your Personal Files – Your Music, Your Pictures or Whatever." *www.techsupportalert.com/content/use-command-line-easily-create-list-your-personal-files-your-music-your-pictures-or-whatever*

IBM. "Database Blocking and Deadlocks." *http://publib.boulder.ibm.com/tividd/td/BSM/SC32-9084-00/en_US/HTML/bsmd240.htm*

Infostor. "Manage Unstructured Data: File Analysis at Scale." *www.infostor.com/storage-management/manage-unstructured-data-file-analysis-at-scale.html*

International Software Testing Qualifications Board. "What are the Software Development Life Cycle (SDLC) phases?" *http://istqbexamcertification.com/what-are-the-software-development-life-cycle-sdlc-phases/*

Jam Software. "Create Lists of Director Contents and File Properties. *www.jam-software.com/filelist/*

Javelin. "Easily find the character length of particular file paths." *www.javelin-tech.com/blog/2011/08/file-path-length/*

Micro Focus. "How can I create a hierarchy in MS Excel using "Group and Outline" when importing requirements using the Office import tool?" *http://community.microfocus.com/borland/test/silk_central/w/knowledge_base/16603.how-can-i-create-a-hierarchy-in-ms-excel-using-group-and-outline-when-importing-requirements-using-the-office-import-tool.aspx*

Microsoft. "Naming Files, Paths, and Namespaces." *https://msdn.microsoft.com/en-ca/library/windows/desktop/aa365247(v=vs.85).aspx#maxpath*

Microsoft. "Understanding and Avoiding Blocking." *https://technet.microsoft.com/en-us/library/aa178087(v=sql.80).aspx*

SharePointGeoff. "How to quickly list documents and sub folders from a Document Library in SharePoint to a file." *www.sharepointgeoff.com/how-to-quickly-list-documents-and-sub-folders-from-a-document-library-in-sharepoint-to-a-file*

Smallwood, Robert. *Managing Electronic Records: Methods, Best Practices and Technologies*. Hoboken, NJ: Wiley, 2013.

Softonic. "JDiskReport" Download. *http://jdiskreport.en.softonic.com*

Windows Club, The. "How to print list of files in folder in Windows 8." *www.thewindowsclub.com/print-list-of-files-in-folder-windows*

South River Technologies. *www.southrivertech.com/*

WebDAV. *www.webdav.org*

Webopedia. "client-server architecture." *www.webopedia.com/TERM/C/client_server_architecture.html*

Benefiting from the **NIST Cybersecurity Framework**

Meg Scofield

"The Framework for Improving Critical Infrastructure Cybersecurity," which was published by the National Institute of Standards and Technology, acts as a Rosetta stone to help organizations translate and navigate among complex cybersecurity requirements. Its adaptability makes it applicable to a broad range of operating environments and potentially will make it the *de facto* industry standard.

Security breaches dominate the news. This past summer, a federal government computer hack compromised personal information belonging to 21.5 million individuals. In September 2014, Home Depot's credit card breach cost the company an estimated $62 million for damage control, like credit monitoring. Then, only a month later, network data bandits targeted Staples and stole more than 1.16 million credit cards.

For organizations, their leaders, and their customers, these incidents can mean professional – as well as personal – devastation. In addition to the significant expense incurred in just responding to a breach, there are financial and time losses resulting from ensuing lawsuits. Not so easily measured is the additional economic damage of the negative publicity.

Ever-increasing volumes of electronic information mean growing vulnerability to cyber-threats. Rather than assume the IT shop is handling the risks, a collaborative effort between IG and IT will best produce a strong information governance (IG) strategy and robust online protection.

The "Framework for Improving Critical Infrastructure Cybersecurity" (Framework), developed in 2014 by the National Institute of Standards and Technology (NIST). provides the common language collaborative parties need to talk about how organizations can keep online information safe.

(A free PDF of the Framework can be downloaded from *www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*.)

A Path Through the Panic

In 2013, President Barack Obama issued Executive Order 13636 that directed NIST to work with government and private industry representatives to create guidelines to help critical infrastructure organizations keep their online platforms safe.

> ...an organization might begin by comparing existing information protection practices with those described in the document.

The order defines *critical infrastructure* as essential systems that, if impaired, would result in "a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Examples include public and private sector areas like utilities, health care, agriculture, chemical manufacturing, and water supply.

NIST, in developing the Framework, convened industry representatives and members of the public and asked what would be valuable for them. A year later, the answer became the Framework document, offering voluntary and technology-neutral precepts for information protection.

The Framework's Broad Relevance

Matt Barrett, NIST program manager for the Framework program, describes the financial services industry as a model that illustrates the Framework's relevance. The Framework has a role in ensuring the security of daily financial transactions like using an ATM machine, swiping a credit card, or making an online purchase.

"When critical infrastructure organizations win, we all win," Barrett says.

Not only critical infrastructure can benefit from using the Framework. NIST's website features use case studies from organizations as varied as Intel and the University of Pittsburgh. In addition, the Framework's reach has expanded to an international audience. A Japanese translation is available, and Italy produced cybersecurity guidance that incorporated the Framework's recommended activities.

NIST also encourages small companies to use the Framework, even if they think they are too insignificant to need to worry about cybersecurity.

Bruce deGrazia, J.D., CISSP, the University of Maryland's University College program chair and collegiate professor, cybersecurity, cautions, "It's what we in the field call *'Security by obscurity.'* The fact that we have a phrase for it indicates that it's not something you can hide behind."

On the other end of the spectrum, while U.S. federal government agencies may adopt Framework activities, they are not required to do so. Mandates and regulations for federal security come from the Federal Information Security Management Act (as amended), the White House Office of Management and Budget, and NIST's own standards and recommendations set forth in federal information processing standards and special publications.

Integrative Approach to Cybersecurity

As Barrett explains, with five functions, 22 categories, and 98 subcategories, the current Framework version 1.0 provides a standardized set of cybersecurity outcomes around which to convene and focus energy. Dialogue about online vulnerability can be internal to an organization, among organizations, or even between an organization and its customers.

In short, the Framework's guidelines can help comprehend and control risks to valuable online assets.

Executive consultant Ren Cahoon, of Reynolds Cahoon LLC (formerly CIO of the National Archives and Records Administration and senior advisor on electronic records to the archivist of the United States), explains the process as incorporating security with everything else that's going on in an organization. He encourages information professionals to use the Framework to become comfortable with cybersecurity – not necessarily to be an expert, but to gain a basic understanding of how cybersecurity contributes to overall governance of information.

Cahoon says, "Before the Framework, there was a lot published, people had a lot to say, but there was [nothing] comprehensive."

Technology Experts Not Required

While NIST is a technical organization, the Framework itself is designed for people who aren't technical experts.

Barrett describes the Framework as "an easy, breezy read," purposely different than a typical NIST publication that is hundreds of pages long and heavy on details. Instead, the Framework document is just under 40 pages long, 17 of which comprise the core body; appendices make up the rest.

Throughout 2015, NIST representatives offered workshops and attended conferences and other events across the country to help explain the Framework. The intent has been to publicize the Framework's components and to make sure that all participants, including those who may not be technologically adept, understand how implementing it can benefit their organizations.

"When it comes to total cybersecurity protection," deGrazia points

out, "the approach and the ability to address problems come from the management side."

Getting Started with the Framework

To use the NIST Framework, an organization might begin by comparing existing information protection practices with those described in the document.

Next, an organization might target areas of improvement. The Framework is not meant to replace successful activities, but to complement ongoing efforts and suggest new areas of focus. The analysis process is designed to be repeated at regular intervals.

The Framework's three sections daylight areas that need strengthening and serve as a guide to building areas that don't exist:

Core: This section outlines the basic functions – Identify, Protect, Detect, Respond, and Recover – that describe at a high level the continuous looping life cycle of cybersecurity activities. The five functions help prioritize resources and promote cybersecurity awareness.

Implementation Tiers: Four tiers (Partial, Risk Informed, Repeatable, and Adaptive) explain the range of risk management practices. Note that the tiers don't represent maturity levels. Moving from one tier to the next is tied to risk reduction and resources.

Profile: An organization can define goals and objectives via self-assessment of the "As-Is" state and the desired "To-Be" state.

Final segments include communicating cybersecurity expectations; adding or revising practices to tailor the guidelines to specific needs; and evaluating how personal information is collected and retained.

Cahoon suggests an organization think about how secure information and data can be managed in a holistic way. "Balance is important, the connection between security and access, between security and continuity of operations, and how retention is managed," he says.

He uses the analogy of building an incredible automobile to illustrate the concept. Bring together in a warehouse the best engineers and cars. From one model, engineers pull out the finest engine and from various other models the finest transmission and the best suspension, sound system, climate control, and so forth, putting them all in the middle of the warehouse. Cahoon explains, this isn't a car – only a pile of parts.

"If an organization is just implementing best practices all over the place, the parts don't fit together any better in an organization than they do in that warehouse with the pile of parts," Cahoon says. "It's a question of deciding what are the right practices for the organization in terms of risk, and integrating those practices in a way that really optimizes and

"The Framework for Improving Critical Infrastructure Cybersecurity"

Benefits	Section Features
Core: Reconciles and clarifies legislation, regulation, policy, and industry best practices	Reduces the time and expense of starting an information security program
Reduces risk within current information security programs by identifying areas for improvement	Core: Guides organization and management of an information security program
Increases efficiencies and reduces miscommunication within an organization and with stakeholders, such as customers, partners, suppliers, regulators, and auditors	Profile: Measures current state and expresses desired state Profile: Enables investment decisions to address gaps in current state Profile: Communicates cybersecurity requirements Tiers: Enables informed discussions of resources vs. risk

Source: National Institute of Standards and Technologies; adapted from a January 2015 NIST presentation, "From Framework to Action: Understanding the NIST Cybersecurity Framework"

tunes the organization to its highest performance."

Potential Benefits of Using the Framework

For Barrett, one of the Framework's advantages is its ability to navigate complex cybersecurity requirements and the operational landscape. "We have a dizzying number of things to help keep us secure," Barrett says. "The Framework acts as a Rosetta stone to translate amongst those."

> The Framework's three sections daylight areas that need strengthening and serve as a guide to building areas that don't exist.

Because of the Framework's adaptability across a range of businesses and fields, deGrazia believes it will become the *de facto* industry standard, and, because of that, may help protect an organization from liability.

If someone tries to sue organizations that have implemented the Framework, deGrazia says the response could be, "Hey, we've got this Framework in place, we've done all the things that were recommended." It makes it easier for [organizations] to defend themselves in court against potential lawsuits."

Considerations for Using the Framework

While cybersecurity should be included as an integral part of how an organization functions, Cahoon recognizes it can also constrain an organization's productivity, even hinder information access.

"In some organizations, security casts a pall and makes doing things so complex and difficult that the costs of that security outpace the risk," Cahoon says. "Organizations mustn't let themselves be bullied by the paranoia around cybersecurity. Be sure cybersecurity is appropriately balanced with all the other important elements of the organization and efforts to accomplish its mission."

Because systems and platforms change frequently, specific technical prescriptions aren't part of the Framework.

Barrett says, "For those who are technically inclined, the Framework could be dissatisfying in that it's not meant to be a 'rubber meets the road' technical approach or methodology. That's on purpose."

Having presented the Framework to technical crowds, Barrett has had to regularly address the value proposition to them. His response?

"When we have things organized over top of that technical echelon," Barrett says, "it leads to efficiency, it leads to lack of confusion, it leads to lack of duplicate work, it leads to less interference from, for instance, evolving cybersecurity requirements, new legislation, new regulation. It enables technical folks to do their job with less drag."

On the other hand, deGrazia acknowledges that putting the approach into place isn't accomplished easily, quickly, or inexpensively.

"The Framework is not something that you can establish once and then walk away," deGrazia says. "It's going to have to be continually reviewed like any other policy would have to be reviewed, and continually updated. So you can't say, on Jan. 1st we've got the Framework in place, we've done everything, and we never have to worry again. I'm not sure that small- to medium-sized businesses recognize this."

For those organizations with limited resources, Cahoon adds another possible concern.

"From a small business perspective, there should be a 'Cybersecurity Framework Lite,' Cahoon says. "If I'm a small business, I'm going to do as much as is necessary to do, and no more. Not try to do so much that – number one – [a small business] can't function, and – number two – can't afford to implement it all. There needs to be something that's streamlined and simplified for the organization that can't afford a major cybersecurity function."

Future Directions

As the dynamic arena of cybersecurity shifts and changes, NIST encourages industry comments on the Framework.

In December 2015, NIST issued a request for information (RFI) asking for public feedback on a possible update to the Framework and what topics it might need to include. NIST also asked questions on future governance of the Framework, including what is the right balance between industry and government ownership of the Framework going forward to ensure maximum positive effect.

On April 6-7, 2016, NIST plans to host a workshop on the Framework in Gaithersburg, Maryland. The event will provide a forum to address topics of discussion from the RFI responses.

"NIST continues to be a convener relative to the Framework," Barrett says. "One of the things that offers the greatest level of value is that the Framework will evolve and improve over time."

That kind of open communication is vital – between NIST and Framework stakeholders, and between organizations' information professionals, business area representatives, legal experts, and senior leadership.

As material continues to be created and managed electronically, the Framework's developing guidelines will serve as an ally to any information owner determined to stay vigilant about managing risk. **END**

Meg Scofield *can be contacted at meg@twocoffeecups.com. See her bio on page 47.*

NOW SHOWING WEB SEMINARS

What's Your Type?

Regardless of how you define yourself, there's a web seminar series for you! Visit the ARMA Bookstore to catch up on what you missed at **ARMA Live! Conference 2015**.

Reg: $479 Pro: $349

View online now!

ARMA INTERNATIONAL BOOKSTORE

www.arma.org/bookstore

Click on "Web Seminars" or search for ARMA 2015

What Organizations Must Know About the 'Right to be Forgotten'

The European Union's (EU) "right to be forgotten" affects not only search engines but any organization that hosts EU citizens' information or does business in the EU. Records and information management professionals who get requests to remove information must understand the factors that should guide their decisions.

Erik Werfel, J.D., IGP, CIPP-US, CISSP, CEDS

The European Union's (EU) right to be forgotten does not apply specifically to Google alone, although reports sometimes suggest it. Rather, the decision in *Google Spain v. AEPD and Mario Costeja González* is the application of a more general right of erasure under the EU's Data Protection Directive of 1995, and the directive applies not just to search engines but to all organizations that control and process EU consumer data. Organizations should therefore be aware of the directive's provisions, particularly if they do business in the EU.

Under the right of access provisions of the directive's Article 12, EU individuals have the right to request that any data controller remove personal data if the information is inaccurate, inadequate, irrelevant, or excessive. Typical applications of this provision might be a request to remove misleading information on an individual's credit report or to remove inaccurate data from medical records. The *Google Spain* decision held that this right is not a right to the removal of records in data sets, but is a more general right to have obsolete information removed.

The Court Decision

In *Google Spain,* a Spanish citizen living in Spain asked that a notice of foreclosure be removed from the website of *La Vanguardia,* the newspaper that had originally published the public notice, and that links to the notice be removed from Google's search engine. The European Court of Justice ruled that *La Vanguardia* need not remove the notice from its site, in part because the notice was published in fulfillment of Spanish law, and because under the principles of the Data Protection Directive, rights to freedom of expression may counterbalance the right to erasure, especially for media companies.

Google Spain declined to be considered a media company. The court found that Google was a data controller under Article 12 and that the information about the fore-

closure was no longer relevant. Google Spain was therefore required to remove all links to the notice.

The EU Court of Justice indicated that Google should consider each request on a case-by-case basis, balancing the public's interest in the information, the data controller's right to free expression, and the individual's right to privacy. It is anticipated that judgement calls will be necessary. According to Google's website on February 10, 2016, the company had approved 42.5% of the 386,038 requests to remove links it had received since it launched its official request process on May 29, 2014.

An EU *directive* describes an aim for the EU that must be implemented in law by member states. With 28 member states implementing distinct laws, there is bound to be inconsistency. An EU *regulation* is enforceable as law in all member states, ensuring consistency. So, in part to ensure consistency and in part to account for changes in information technology since 1995, the EU recently reached agreement in principle on a new General Data Protection Regulation (GDPR). The GDPR was expected to receive formal adoption from the European Parliament and Council in early 2016, with an effective date sometime in 2018.

Criteria for Erasure

Notably, with regard to the right to erasure, the current Data Protection Directive provides that data controllers must make every effort to inform third parties with whom they share data if any data must be removed because it is inaccurate or irrelevant, while the upcoming GDPR makes data controllers responsible for ensuring that third parties actually remove the information. Organizations that receive take-down requests should consider the following factors in determining whether to comply with each request.

Location

Before removing data, the organization should determine whether the server is physically located in the EU, whether the data processing happens in Europe, or whether the organization does business in the EU. If the answer to all of these is *no*, the directive's provisions do not apply. The court in *Google Spain* held that while the data processing done by Google took place wholly outside the EU, the Spanish subsidiary was selling advertising in Spain, and since advertising was Google's major source of revenue, Google could be considered to be doing business in Spain.

Google has applied the *Google Spain* ruling by providing a form that allows users to request that links be removed. Once the request is approved, Google removes links from all of its European sites (*google.es* or *google.uk*, for example) but not from the U.S. *google.com* site, which is accessible in Europe. The French data protection agency has objected, claiming it makes the information too easily accessible in Europe, and has requested that the links be removed from *google.com* as well.

It might be possible for an organization to use a technological solution to remove the links for end users based on the location of the source Internet protocol address (which could possibly be spoofed) or a more creative solution similar to Google's. But a sure way for an organization to comply with a legitimate request is to remove the information globally.

...the current Data Protection Directive provides that data controllers must make every effort to inform third parties with whom they share data if any data must be removed because it is inaccurate or irrelevant.

Data Controller

As provided by the Data Protection Directive, a *data controller* "determines the purposes and means of the personal data processing." Data an organization is hosting for someone else might not be data it controls.

Identification

The right to erasure is a personal right, so persons making a request must be able to demonstrate that they are the persons whose rights are implicated or that they have the approval of the person whose rights are implicated. Google requires some form of photo ID before it will approve requests for removal, and it is reasonable for other organizations to require some sort of documentation of identity before approving or considering a request.

Balance of Rights

The Data Protection Directive indicates that the individual's right to privacy must be weighed against the publisher's right to free expression and the community's right to know. As generally applied, media companies have not been expected to comply with requests to remove

Criteria for Determining the Need to Comply with a 'Right to Be Forgotten' Request

"Yes" answers to these questions indicate the liklihood that the requested information should be removed:

- Is the server housing your data located in the EU, is the data processed in the EU, or does your company do business in the EU?
- Is your organization the data controller?
- Is your organization something other than a media company?
- Has the requester provided documentation proving that he or she is the person whose rights are implicated OR that he or she has the approval of the person whose rights are implicated?
- Is the data inaccurate, inadequate, irrelevant, or excessive?

information, and provisions in the proposed GDPR would make media companies explicitly exempt once that regulation is adopted.

So, it may be safe to assume that newspapers and media companies do not need to consider take-down requests. Google Spain opted not to be treated as a media company, so no ruling on that point was required in the *Google Spain* decision, leaving open the possibility that "media company" may be broadly defined. As an example of the varied ways European media companies are applying the directive, some European newspapers host pages displaying the stories for which Google has removed links from its search results in response to right to be forgotten requests.

Relevance of Information

Determine whether the information is inaccurate, inadequate, irrelevant, or excessive. In the *Google Spain* decision, the information that was the subject of the case was accurate, in that the foreclosure had taken place. However, Costeja was no longer insolvent, and he argued successfully that the notices did not reflect his current condition and were therefore irrelevant because the information was obsolete.

Truth alone would not be a reason to deny a request to remove information, and indeed it is because accurate information may be removed that this provision is known as the *right to be forgotten*, rather than *the right to correction*.

Penalties for Non-Compliance

Under the Data Protection Directive, the implementing law sets fines for noncompliance, so the cost of noncompliance is not consistent across the EU. Under the new GDRP, a fine may be levied up to €20 million ($2.4 million U.S.) or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

The costs can be substantial, so this should be factored into an organization's decision about whether to comply with a takedown request. On the other hand, there is generally an appeals process with the member state's data protection authority, and an initial ruling is more likely to order the removal of information than a fine.

Invoking the Right to Protect Reputation

Organizations should bear in mind that while the EU's right to be forgotten is an individual right, it may be that invoking the right to be forgotten to enhance the reputation of a key individual would benefit the organization as a whole. Records and information management professionals should be able to recommend and assist with requesting the removal of information from third-party sites, if that is appropriate.

An appropriate request for removal will meet these criteria: the site should be hosted in the EU or the host company should be doing business in the EU; users should be in the EU; the host in most instances should not be a media company; and the information should be inaccurate, inadequate, irrelevant, or excessive.

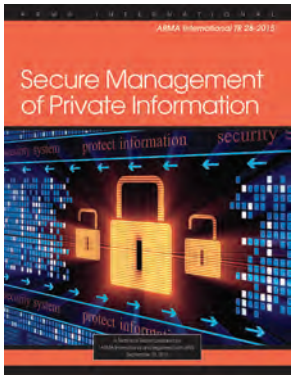
Prospects for a Similar U.S. Right

Privacy advocates, including, for example, the often-cited Eric Posner of the University of Chicago Law School, have argued there should be a similar right to be forgotten in the United States. However, while the EU's right to be forgotten requires that the individual's right to privacy be balanced against rights of free expression, it seems likely the U.S. First Amendment would not allow the prohibition of publication of information that has not already been found defamatory by a court.

Many states already allow a tort claim for public disclosure of private facts, and perhaps that might be a model for applying the right in the United States, requiring adjudication for removal. But courts typically rule narrowly on claims for public disclosure of private facts, in recognition of First Amendment interests, which suggests they would be reluctant to extend rights under such a claim any further. A U.S. right to be forgotten would need to be very different in form from the EU's, and might nevertheless be constitutionally suspect, so it seems unlikely such a right would be adopted in the near future. **END**

Erik Werfel, J.D., IGP, CIPP-US, CISSP, CEDS, *can be contacted at erik.werfel@gmail.com.* *See his bio on page 47.*

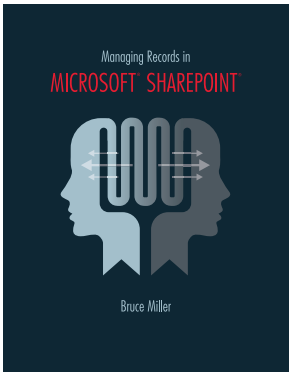
Resources for Advancing Your Career



Secure Management of Private Information (ARMA International TR 28-2015)

This technical report identifies the risks associated with private information, provides policies, tools, and techniques for mitigating them, and tells how to audit for compliance with privacy policies.

A4968 **$60.00** Professional members: **$40.00**
V4968 PDF **$55.00** Professional members: **$35.00**

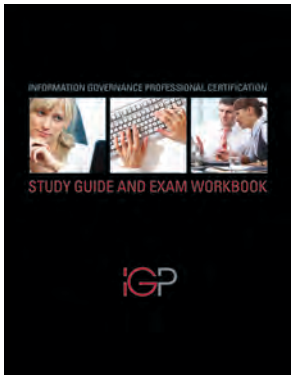


Managing Records in Microsoft® Sharepoint®

Bruce Miller

This book examines SharePoint's® native recordkeeping capability's shortcomings and explains how to optimally deploy third-party recordkeeping technology to overcome them.

A5024 **$85.00** Professional members: **$60.00**
V5025 PDF **$80.00** Professional members: **$55.00**



Information Governance Professional Certification: Study Guide and Exam Workbook

This PDF study guide will help you develop and execute your preparation plan for taking the IGP certification exam. It provides a self-assessment tool that will help you identify content areas where you need to focus your study and suggested resources to help you learn more about each of those areas.

V5028 PDF **$75.00** Professional members: **$50.00**

Order online today! **ARMA INTERNATIONAL BOOKSTORE**

www.arma.org/bookstore

In Search of an Effective RIM or IG Program

Fred Diers, CRM, FAI

Does an effective enterprise records and information management (RIM) or information governance (IG) program really exist?

There are many articles, webinars, educational seminars, and champions professing the need for and benefits of a compliant RIM program – which, as the core of IG, is a prerequisite for an effective IG program. ARMA International even offers a measurement tool based on the Generally Accepted Recordkeeping Principles® that enables RIM and IG professionals to assess the maturity of their organizations' programs so they can identify and foster needed improvements.

Yet, in working with and observing hundreds of RIM and IG programs during more than 40 years of consulting and speaking engagements, this author has never found a single sustainable and compliant enterprise program. Based on this, he contends that there are *no* functioning, enterprise-wide programs that set standards and rules that personnel are required to follow – period!

The State of RIM Programs

RIM and IG professionals may take exception to the above statement. Many will respond that their organizations have RIM and IG policies and records retention schedules that are available to all employees. Others may argue that they have annual information disposition days where personnel clean up their work areas and dispose of information. Still other program champions may promote their programs as compliant and risk avoidant to their executives or board.

But, if these statements are true, why do so many organizations have:

- Outdated policies and records retention schedules
- Retention schedules that do not reflect the organization's structure or the information it creates, distributes, and retains
- Personnel who know little or nothing about the policies or records retention schedule – or believe they are for those who deal with the paper records in offsite storage and do not affect them
- No continuous education or training on policies and procedures

- No auditing to ensure up-to-date program compliance

Some may argue that these conditions are not representative of most organizations – that most RIM programs are working to the satisfaction of management. But, the on-going demand for experienced RIM and IG professionals/consultants to update policies and retention schedules and to automate RIM processes – from organizations private and public, large and mid-size, and with national and international footprints – refutes that.

Let's look, then, at why so many organizations don't have a compliant and sustainable RIM or IG program.

Obstacles to Effective RIM and IG Programs

Some reasons for poor RIM and IG program implementation and sustainability are:

- Change in management structure and loss of the program champion
- Lack of staff accountability
- Complicated retention guidelines
- Lack of management support for the RIM program manager
- Enterprise content management tools that are not used as enterprise solutions or repositories
- No enterprise taxonomy standardizing terminology, indexing, media, or ownership
- An out-of-sight, out-of-mind mentality
- Lack of understanding what a RIM program is
- Humans' inherent resistance to change

Resistance to Change Is Major Factor

The final listed item is the main reason organizations are struggling to implement effective RIM and IG programs. Resistance to change is especially evident in managers who fail to see the benefit in disrupting their staff's work routines with programs they believe contribute little to the financial bottom line.

The result of this resistance to change is clearly demonstrated in the following scenarios, which are mirrored by the majority of companies.

No Enforcement, Compliance

A newly hired general counsel (GC) is critical of the organization's out-of-date, 10-year-old retention schedule. Due to legal holds, the records policy and schedule had been ignored by the previous counsel. Since the new GC wants realistic RIM and IG policies reflecting the company's digital environment, he hires a RIM and IG consultant to update the program.

The consultant collects data, interviews stakeholders, creates taxonomies, revises policies, and develops a compliant, realistic retention schedule. The consultant's presentation about the new program structure and its associated policies and schedule to the GC and the management team introduces:

- The lifecycle position of managing company information assets at the point of creation with indexing standards and rules
- Tools to assist personnel in processing and retaining their documents
- Policies for enforcing compliance through audits and performance penalties

Upon the presentation's completion, the GC's immediate response is, "This program proposal will force too much change on the company and its personnel. Just provide a retention schedule that can be issued for the staff to follow."

As a result, this company will have a policy-driven program with "no teeth" to ensure compliance and sustainability – and the prospect that in 10 years it will update the policies and retention schedule again and continue operating under the false assumption that staff will voluntarily comply.

Partial Deployment

An organization employs hundreds of Microsoft® SharePoint® sites for various departments to use to manage their projects' digital information. With Microsoft continually updating and adding enterprise capabilities to SharePoint, the IT department has the opportunity to turn on standard "content descriptions and record center" functionality.

When asked why IT does not implement this enterprise functionality to universally manage digital records, IT staff respond, "It creates too much change for the user and will necessitate adding full-time SharePoint administrators."

> Focusing on communication, education, and careful technology deployment will help personnel make the changes necessary...

No Compliance Auditing

A large, heavily regulated organization reorganizes and wants to move the RIM program to the facilities department because it is perceived as a warehouse function, simply managing paper documents in offsite storage. A program assessment finds an outdated, department-based retention schedule and RIM policy that the majority of personnel ignore. In fact, the only recollection personnel have of the RIM policy is from their new employee orientation where they were asked to review all company policies and sign an acknowledgement form.

Although the RIM policy clearly states that the schedule is to be used to manage and dispose of paper and electronic records, it is used only to destroy paper records in storage; identifying and disposing of electronic doc-

uments from shared drives and e-mail are perceived as too time-consuming and non-productive.

Pockets of Compliance

While resistance to change often causes RIM programs to fail at the enterprise level, there are pockets of compliance with RIM and IG policies and RIM procedures in many organizations. Adherence is usually found in individual departments or in locations that are externally audited by ISO or government agencies.

For example, if U.S. Nuclear Regulatory Agency (NRA) auditors cannot access specific documents or if those documents are not appropriately maintained in certain parts of a nuclear energy company, NRA auditors can shut down the power plant, creating a major crisis for the parent company. Yet in the company's administrative office environment, resistance to change is often evidenced by inconsistent application of policy.

How to Overcome Resistance to Change

Focusing on communication, education, and careful technology deployment will help personnel make the changes necessary for implementing and sustaining an effective RIM program.

Communicate: from the Top Down

Minimizing resistance starts with communication from the top executive down that constantly and consistently reinforces that compliance with RIM and IG policies and related RIM procedures is mandatory. This will dispel staff fears that management will not accept them destroying information in accordance with the retention schedule and that they will suffer consequences if they do; these fears may be causing staff to ignore policies and retain information "just in case" management needs it.

Educate Senior Management

Senior management must understand the RIM program's purpose – that it is not just about e-discovery or legal holds, but it also drives standards that:

- Enable authorized personnel to access complete and accurate information easily
- Reduce information volumes
- Instill confidence in information disposition
- Minimize legal and operational risks

Senior management also must understand from program conception:

- RIM and IG policies and the retention schedule are corporate standards that are not open to interpretation once approved by the organization's top level of authority, and these standards must be supported at all levels.
- The policies and retention schedule are living documents that must be reviewed and updated annually.
- Implementing the procedures related to the policies and retention schedule *will* result in changes to how staff process and handle information, from its creation through disposition. The gravity of the change can be diminished by an ongoing resource commitment, including for:
  - An application to assist users in creating, sharing, and storing information assets
  - A single repository for final versioning of corporate documents
  - Effective staff education and "town hall" meetings where personnel have input into the design of policy-driven standards and rules
  - Continuous user assistance
  - Audits to test the effectiveness of and compliance with the policies and retention schedule

> ...fears may be causing staff to ignore policies and retain information "just in case" managment needs it.

Partner with IT

Introducing technology also often creates resistance to change. An IT department that is eager to respond to users' requests for new applications to make their work environment more efficient may introduce applications without standard rules for their use; deploy applications to meet a specific user or group's requirements, rather than enterprise-wide applications; and leave it to users to set up, index, and control enterprise-wide applications and tools, such as e-mail and shared drives.

These actions allow users to develop bad information-processing habits that affect their compliance with RIM and IG policies and the records retention schedule. It is then necessary to change the users' behavior, and managers may opt to avoid this effort rather than disturb the status quo.

To prevent these bad habits and minimize the need for changing user behavior, RIM must partner with IT to ensure that any new application or document repository is designed to allow conformance to the standards and rules provided in the policies, RIM taxonomy, and retention schedule.

The program standards and rules come first, not the technology.

Elements of Effective Programs

To have effective, enterprise-wide RIM and IG programs, their scope must include the lifecycle processing

of the organization's information assets. This requires:

- IG policies, which are strategic in nature, that conform to management objectives and the organization's culture
- Mandated adherence to RIM and IG policies, in the same way that adherence to other corporate policies is mandated and compliance with them is monitored and enforced
- An enterprise application that has policy and retention standards and rules imbedded in its administrative tables and is accessible throughout the organization for users to create, capture, share, distribute, retain, and dispose of digital and physical information
- A retention schedule that is easy to use and has realistic retention values. The day of 100-page retention schedules is over; big bucket categorization is required in this digital world.
- Annual updates of policies and the retention schedule
- Ongoing user support and education to reduce resistance and help ensure acceptance and compliance with the policies

Sell the RIM Program

Change is inevitable. The role RIM plays is dependent on management commitment and their understanding of what elements an effective enterprise RIM program comprises.

If RIM and IG professionals can strategically sell these elements, then change can be managed, rather than be a roadblock to the program's success.

The search for a sustainable, effective, enterprise RIM or IG program goes on.... **END**

Fred V. Diers, CRM, FAI, can be contacted at fdiers@msn.com. See his bio on page 47.

Seven Things

Records Destruction Vendors Are Afraid to Tell You

Robert (Bob) Johnson

Information management service providers are often presented with a dilemma. On one hand, they have to give customers what they want. There are many competitive options out there, and service providers need happy customers. On the other hand, they have (or should have) considerably more experience and training than their typical customer and sometimes know that what a customer wants isn't prudent.

Faced with this conflict, most service providers do not speak up for fear of offending a current or potential customer. They feel it is far less dangerous to just agree; it is difficult to tell the emperor he has no clothes. The unfortunate side of this is that customers remain unaware (or in denial) about factors that put them at risk.

Here are seven things organizations should know that secure destruction service providers want to tell them – but probably don't.

1 Don't Depend on Employee Compliance

"Quit letting every employee decide what information needs to be destroyed."

The typical data destruction program falls into two main categories:

1. The organization places a bunch of shredders around, instructing employees to use them to destroy confidential or regulated information.
2. The organization hires a service to destroy confidential and regulated information, instructing employees to place it into some type of secure collection container.

The common problem with both programs is that they rely on employees' discretion and discipline. If they forget or ignore their responsibility and instead put this information – on paper or on electronic media, such as thumb drives, handhelds, and laptops – in the trash or recycling bin, the information is at high risk for exposure and, depending on the information, the organization could be in violation of regulatory mandates.

Frankly, it makes no sense to give every employee the capability to put the organization's reputation, compliance, and profits at risk in this manner. No organization would consider giving every employee the discretion to bypass its firewalls, so it should not give them the discretion to undermine security, compliance, and client trust because they are too busy, too lazy, or too apathetic to properly dispose of protected information.

The secure and compliant solution is to remove employee discretion from the equation by destroying all discarded media. Given the relatively low economic commitment, especially compared to the cost of the potentially devastating consequences, destroying all discarded media is the only sensible choice.

The secure and compliant solution [for the proper disposal of confidential or regulated information] is to remove employee discretion from the equation by destroying all discarded media.

2 Destroy All Media When It Is Time to Discard It

"You should have the same consistently high standards for the destruction of all types of media."

Destruction methods vary for each type of media, as does the oversight of each destruction process. For instance, stored paper records usually fall under records management's responsibilities, while the destruction of the daily flow of incidental records (e.g., paper, thumb drives) out of the organization is often considered a facilities management issue. And, when information technology (IT) assets, such as old computers or other IT hardware, are discarded, it typically falls to the IT department.

Data destruction service providers, who handle all of these forms of media in the course of their operations, often find customers are extremely conscientious about securely disposing of some forms of media but completely negligent in disposing of others. It might be that stored records are destroyed responsibly, while the daily, real-time, confidential materials are just tossed out with the trash, and computers containing information that should be protected are sent to a scrap recycler with no thought at all about the data on them.

The fact that one department treats information disposal responsibly establishes that the organization realizes its legal responsibility and exhibits acceptable behavior. So, when another department within that organization ignores this responsibility, the organization is considered negligent. The solution is a consistent standard for the proper destruction of all media forms under one, uniform, written policy, along with regular monitoring for compliance and enforcement. (See number 4 below for more about this.)

3 Get Real About Liability

"You need to align your service providers' liability with their professional indemnification."

The liability and damaging consequences of a data security breach are increasing dramatically. Because customers usually are held responsible for the data security breaches caused by their services providers, it has become a best practice for those customers to hold service providers liable for any such damages. By signing a contract that assigns them this liability, service providers accept it.

Unfortunately, organizations often fail to ensure that their service providers have the right indemnification in place to cover that liability; that is, they don't:

1. Check vendors' liability coverage
2. Understand that vendors' general business liability coverage is not sufficient
3. Use vendors that have professional errors and omissions liability coverage that is designed specifically to address data-related risks, rather than some off-the-shelf professional liability coverage

If regulators discover that a data security breach was caused by a service provider that was selected only on the criterion of price, they will find the organization in violation of the law.

This brings up another common customer behavior that should be challenged: attempting to transfer unlimited liability. It is never in the customer's interest to transfer a liability for which the service provider indemnifies. No service provider can obtain indemnification for an unlimited amount. Since the customer is ultimately only protected to the amount of the indemnification, setting liability higher is only a mirage anyway. Organizations are best protected when contracts set a reasonable amount of liability for service providers and make sure the proper coverage is in place.

4 Take Advantage of Us (We Want to Help)

"Let us do the two simple things that can help insulate your organization from the consequences of a data breach."

Many data destruction service providers have the capability to provide clients with written procedures and employee training that minimize the impact of a data disposal breach (see number 2 above), and yet most customers don't take advantage of it.

It might surprise readers to know that the regulators enforcing data protection requirements are likely to be more lenient with data breach punishment when an organization has done what it can do to secure its data – like establishing data protection policies, procedures, and training – and harsher when it has not; they understand there are some things an organization can't control.

When the Health Insurance Portability and Accountability Act (HIPAA) was amended in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act, a mandatory fine scheme was created, with the most egregious and expensive violation being for an organization's "willful neglect" of its compliance requirements. With the associated mandatory fines being increased by 6,000%, the U.S. Department of Health and Human Services (HHS) thought it useful to provide examples of violations rising to this most severe level.

The first example HHS offers describes a situation in which protected health information is discovered casually discarded in a dumpster. An investigation reveals that the offending organization has no written disposal policy and no employee training. In this situation, HHS states, it is not so much the violation that would constitute willful neglect; it is the lack of written procedures and employee training that does.

A breach that occurs because an employee ignores training and violates written policies and procedures places less fault on the organization than one that occurs because the organization did not provide policies, procedures, and training. This is why every data protection regulation in the world includes a requirement to have written procedures and employee training.

So, if service providers can provide tools that minimize the risk of a breach, comply with the law, and help insulate an organization from the worst sanctions at little or no charge, the organization should take advantage of it.

5 Don't Be a Cheapskate

"It is illegal to select a service provider based on its price alone."

Every data protection regulation in the world – HIPAA and Canda's Personal Information Protection and Electronic Document Act, for example – requires customers to demonstrate that any service provider accessing regulated information has the appropriate security and regulatory qualifications to do so. One of the ways regulators enforce this requirement is to hold the customer responsible for the actions of those vendors. So, if regulators discover that a data security breach was caused by a service provider that was selected only on the criterion of price, they will find the organization in violation of the law.

This requirement to conduct due diligence in selecting a service provider can be challenging because ensuring secure destruction is a very small fraction of the job for the vast majority of decision makers. They simply don't have the time or wherewithal to learn all they need to know and perform their due diligence by verifying and monitoring the truth of what a service provider has told them.

This is where industry certifications, which were formerly used simply to provide peace of mind, now assume a much more important role. An industry certification issued by a certifying body that verifies and monitors the regulatory compliance of those who earn the certification provides the due diligence an organization would otherwise have to do itself. Therefore, an organization that requires service provider candidates to have that industry certification ensures its own regulatory compliance.

Of course, this means organizations have to do their due diligence in

confirming and monitoring the validity of the industry certifications they require of service providers. Because organizations are turning to certifications as a way to confirm vendor compliance, many more organizations are offering industry certifications. Some of these are inadequate, issued by organizations that do little in the way of verification; sometimes they require no more than the submission of paperwork and a small fee.

So, while proper certifications can do the heavy lifting on vendor due diligence, organizations must perform due diligence on the certifications themselves to determine which ones they require.

6 Pay Attention to IT Assets

"You cannot afford to ignore the fact that IT assets are missing."

When organizations reconcile IT assets being retired from use after they are depreciated, it is not uncommon to discover a significant percentage missing.

Last year, for example, Coca-Cola notified thousands of past and present employees that their personal information was at risk when IT equipment potentially storing their data could not be located during just such a reconciliation. The most unique aspect of Coca-Cola's action was that in notifying those affected, the company actually did what it was supposed to do.

In contrast, most companies either ignore missing IT assets or do no reconciliation at all. Should one of those missing IT assets turn up on the second-hand market later, it would create a major public relations and regulatory headache. There is no statutory limitation to this liability; therefore, it exists in perpetuity – like a landmine that could go off at any time.

If an organization does nothing else, it should document the fact that IT assets cannot be found. In an incident report, list the items, the information thought to be on those items, the steps taken to determine the nature of the information, the circumstances surrounding the equipment's disappearance, and how the situation was resolved, including details about the possible breach notification and remedial steps taken to prevent this type of incident from recurring. By this, the organization can show it reacted appropriately if one of these landmines goes off later.

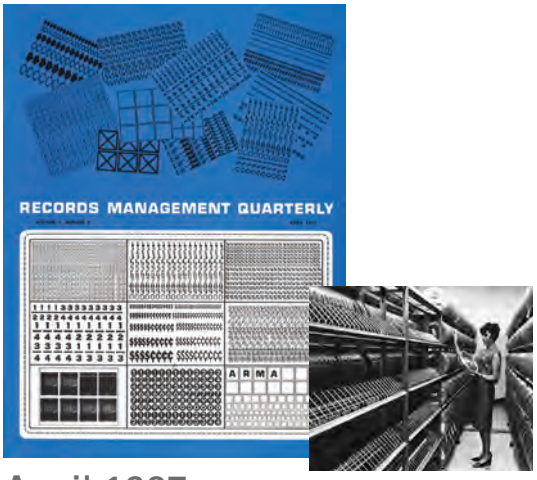
Of course, the real solution is to prevent this situation by better tracking IT assets from acquisition through retirement.

7 Act Now

Organizations that act on these six recommendations that records destruction providers want to give their clients – but don't for fear of offending them – will ensure both the secure disposal of their protected information and a strong partnership with their service provider. Best of all, taking these steps requires little to no additional cost. **END**

Robert (Bob) Johnson *can be contacted at rjohnson@naidonline.org. See his bio on page 47.*

50, 25, 10 Years
Looking Back...



Magnetic tapes, circa 1967.

April 1967
Records Management Quarterly

Association News

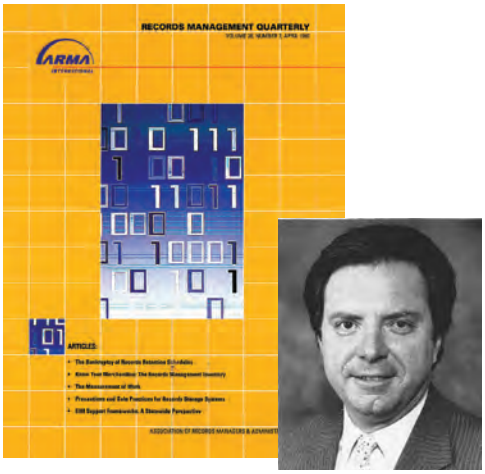
- American Records Management Association's (ARMA National) headquarters is located at 738 Builders Exchange, Minneapolis, MN.
- The president of ARMA National is Eunice Thompson.
- ARMA's 12th annual conference is scheduled for Oct. 24-27, 1967, at Hotel Roosevelt in New York City.
- The Business Forms Management Association considers affiliation with ARMA National.

Articles

- "Counseling the Computer User" by Robert P. Bigelow
- "The Effects of EDP [electronic data processing] on Records Management" by John W. Porter
- "Documenting Computer Operations" by Everett O. Alldredge
- "Impede or Succeed" by Hope V. Trombley
- "Forms Design and Procurement" by R.E. Carpenter
- "Investigative Techniques – Surveys and Audits" by Terry Beach
- "Systems Analysis and Work Simplification for Information Management" by Dr. Roger H. Nelson
- "Admissibility of Videotape Copies of Documents in Evidence" (no author named)
- *Automated Data Processing,* by Frederick P. Brooks, Jr. and Kenneth E. Iverson, was reviewed by Charles Macbeth.

Advertising

This second issue of *Records Management Quarterly* contained no advertising.



Fred Diers (1992) also wrote an article for this issue of ***IM.***

April 1992
Records Management Quarterly

Association News

- ARMA headquarters is located at 4200 Somerset Dr., Ste. 215, in Prairie Village, KS.
- The president of ARMA International is Manker R. Harris, CRM.
- ARMA's new home study course, *An Introduction to Records and Information Management,* is $200 for members.
- Congratulations to our Chapters of the Year: Atlanta, Puget Sound, Greater Topeka.
- Don't miss the 37th Annual Conference, "Shaping the Information Age," which is to be held October 19-22, 1992, in Detroit.

Articles

- "The Bankruptcy of Records Retention Schedules" by Fred V. Diers, CRM
- "Know Your Merchandise: The Records Management Inventory" by Alice Gannon, CRM
- "The Measurement of Work" by Fraser Boyd
- "Precautions and Safe Practices for Records Storage Systems" by Don Lemley

- "EIM [electronic image management] Support Frameworks, A Statewide Perspective" by James J. Fruscione, CRM
- *Keeping Data: Papers From a Workshop on Appraising Computer-Based Records,* by Barbara Reed and David Roberts, was reviewed by Kenneth V. Hayes.

Advertising

- Canon – ALLBASE+ software connects to the CANNONFILE 250 optical disk filing system
- Information Requirements Clearinghouse – "The Law Library for Records Managers"
- Iron Mountain – "For All Your Records Storage and Management Needs"
- O'Neil Software – "Over 300 companies, with over 100 million files, trust their records to O'Neil. *Shouldn't you*?"
- REB Steel Equipment Corp – "REB Steel…a Reputation for Quality"
- Redweld – "Filing System Specialists" featuring recycled products
- Underground Vaults & Storage, Inc. – "Where do you think you'll find your vital records? …at our fingertips, safe and sound, 54 stories underground."

Iron Mountain has been a long-time supporter.

.

April 2007
The Information Management Journal

Association News

- ARMA headquarters is located at 13725 W. 109th St., Ste. 101, Lenexa, KS
- The president of ARMA International is Susan McKinney, CRM.
- Kick off your RIM Month promotion with these marketing tools from ARMA International: *Records@Work* pamphlets, posters, training materials, web seminars. Visit *www.arma.org/promoteRIM* for these and other materials now available.
- Hot off the Press! *Records Management Responsibility in Litigation Support"* by ARMA International Standards Development Program workgroup and *Records Management: Making the Transition from Paper to Electronic* by David O. Stephens, CRM

Articles

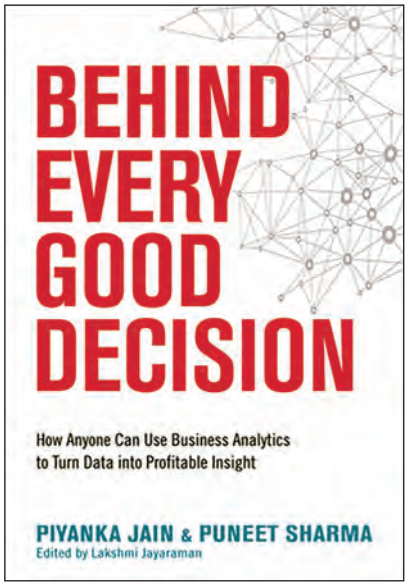
- "RIM Health Check: Auditing an Organization's RIM Program" by Janice Anderson
- "The RIM Manager's Role in Supporting Major Business Changes" by John T. Phillips, CRM, FAI
- "Strategies for Merging Recordkeeping Systems" by Jason Pearce and Bernadette Resnik
- "DIRKS: Putting *ISO 15489* to Work" by Stephen Macintosh and Lynne Real
- "Digital Conversion Projects: A Decision-Making Checklist" by Bud Porter-Roth
- *Understanding Archives & Manuscripts,* edited by James M. O'Toole & Richard J. Cox, was reviewed by Gary Cox, C.A.

Advertising

- Access Sciences – "Access Sciences…Connecting the Dots"
- DHS Worldwide Software – "Experience the most flexible and comprehensive records management software in the world."
- Fujitsu – "Fujitsu scanners. You'll see productivity everywhere you look."
- Institute of Certified Records Managers – "Today's records manager…needs more!"
- NAID – "Choosing a secure shredding service? Heads or tails may not be the best criteria…"
- The Paige Company – "Ordinary boxes hold stuff. Ours are built to hold your future."
- Zasio – "When it comes to managing your electronic records, you'd be happy if *Point-Click-Save* were all it took. With Zasio, it is!" **END**

Analytics Is for Everyone

Judy Vasek Sitton, CRM



This book sets out to accomplish the lofty goal of moving analytics from a vague, overwhelming, and complex discipline – usually associated with big data and predictive analysis – to a simple tool that anyone can use for making smarter decisions. In the process the authors present and explain BADIR™, a trademarked five-step approach to utilizing data for business impact. The acronym stands for:

1. Business question
2. Analysis plan
3. Data collection
4. Insights
5. Recommendations

The authors then show how to tie analytics to return on investment.

The assertions throughout the book are that the use of analytics, except in rare cases, is not rocket science and that analytics is not just about data itself but about using data to guide actions. The authors state that "Unless analytics drive business impact, it is not analytics. It is just statistics; just data science."

Target Audience

In the introduction, the authors identify who this book is for and list specific sections beneficial for that target audience. They show how the book is practical for:

- Everyone
- People who want to learn hands-on analytics
- Leaders

However, if you are looking for more insight into using analytics and big data, look elsewhere. The authors specifically state, "Big Data is NOT synonymous with analytics and we will NOT talk about Big Data in this book. We will talk about how smarter decisions can be made using the data to which you have access."

Organization

Behind Every Good Decision is organized into four sections.

"Hello Analytics!" explains analytics and goes into detail about its various types.

"Diving Deep" delves into analytic tools, including the five-step process and predictive analytics.

"Leadership Toolkit" is self-explanatory.

"Analytics at Work" wraps up the book with 10 case studies that illustrate the use of analytics in diverse settings.

For RIM Pros

The entire book will be of interest to records and information management (RIM) professionals as business leaders. It gives insights on business processes, in general, and talks about how 70%-80% of business decisions can be accomplished effectively with simple analytic techniques and a spreadsheet.

Persons working with internal data scientists or with vendors doing predictive coding of data sets will also find information useful to them in this book. An entire chapter is devoted specifically to predictive analysis and explanations of how the past predicts the future.

Although the examples given lean more toward external marketing than internal use analytics, the common predictive techniques, applications, terminology, and modeling information provided help break down a complex process into bite-size pieces.

The chapter called "Common Pitfalls" is one we can all use.

Behind Every Good Decision: How Anyone Can Use Business Analytics to Turn Data into Profitable Insight
Authors: Piyanka Jain, Puneet Sharma
Publisher: AMACOM Books
Publication Date: 2014
Length: 256 pages
Price: $27.95
ISBN: 978-0-8144-4921-9
Source: *www.amacombooks.com*

Overall Evaluation

I would recommend *Behind Every Good Decision* to ARMA members and other RIM professionals. Though not what I would call an easy read, the book is well written and organized in an easy-to-follow format. The au-

thors have impressive backgronds with complmentary experience in utilizing analytics. They are careful to include the human side of analytics and acknowledge the people skills needed to prepare business counterparts for action.

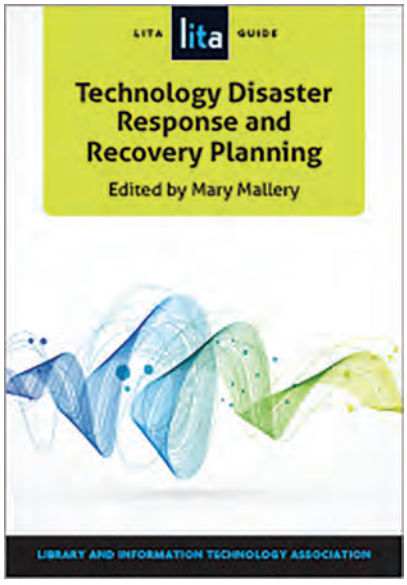
The book provides an understandable framework of the different types of analytics used in business decision making. There is liberal use of charts, illustrations, and models. The case studies at the end reinforce the concepts from the other sections.

Although *Behind Every Good Decision* is focused on applying analytics for results, no prior understanding or experience with analytics is necessary for readers to derive value from this book. **END**

Judy Vasek Sitton, CRM, *can be contacted at* Judy_Sitton@kindermorgan.com. *See her bio on page 47.*

How to Prepare for **Techmageddon**

Crista Bradley



While no one in the information professions can dispute the value and significance of disaster planning, this important activity often ends up getting put on a back burner in a work-day of competing priorities and limited budgets. *Technology Disaster Response and Recovery Planning* serves as a poignant reminder of why the development and regular refreshing of disaster plans need to be incorporated into an organization's regular cycle of work.

The compact guide from the Library and Information Technology Association (LITA) features seven well-considered articles in chapter form that can serve as a useful launch pad for professionals ready to engage in the process of creating or updating their organization's technology disaster plan.

Mallery has assembled a significant amount of information in a slim volume. The book is divided into two parts that, in total, contain seven stand-alone chapters. This arrangement helps make the book a very accessible read.

Creating the Plan

The five chapters in part one, "Creating the Technology Disaster Response and Recovery Plan," expose readers to a range of issues.

Chapter one is Mallery's own, entitled "What Could Go Wrong? Libraries, Technology, and Murphy's Law." It serves to frame the discussion that unfolds in the chapters that follow.

Chapter two, "Inventory and Risk Assessment for Digital Collections" (Liz Bishoff and Thomas F.R. Clareson) encourages readers to take full stock of their assets and risks at the outset of the planning process.

This is followed by "Disaster Planning and Risk Management with dPlan" (Donia Conn), which provides an overview of an online disaster planning tool developed by the Northeast Document Conservation Centre and the Massachusetts Board of Library Commissioners to streamline and support disaster planning.

Next comes chapter four, "Disaster Communication: Planning and Executing a Response" (Denise O'Shea), which prompts those engaged in disaster planning to give careful consideration to the importance of communication in a crisis situation.

The final chapter of part one is also the meatiest, "Future Trends: Cloud Computing and Disaster Mitigation" (Marshall Breeding). It briefly surveys some of the types of library

Technology Disaster Response and Recovery Planning: A LITA Guide
Editor: Mary Mallery
Publisher: American Library Association
Publication Date: 2015
Length: 120 pages
Price: $59
ISBN: 978-0-8389-1315-4
Source: *www.ala.org*

products available in a cloud environment and then considers various cloud service models, approaches, and issues from a disaster planning perspective.

Learning from Case Studies

Part Two, "Managing Techmageddon: Disaster Mitigation and Lessons Learned," includes two chapters featuring interesting case studies on several institutions that confronted significant, recent-memory disasters. The first, "The University of Iowa and the Flood of 2008: A Case Study" (Paul A. Soderdahl), steps through the experience of an institution with a significant disaster. It contains five pages of concrete lessons learned and observations at the end of the discussion that are particularly useful.

The author clearly states that the technical elements of an institutional plan are less important than the context that surrounds them:

> The major takeaway from both the 2008 flood and the 2013 near-miss is the extent to which a library IT disaster response plan is not a particularly valuable technical resource. Certainly, a plan needs sufficient detail to make sense to an IT professional unfamiliar with the environment. But IT professionals solve IT problems for a living, so trying to solve imaginary problems ahead of time should not be a priority. Rather, the most indispensable sections of the plan document the default solutions to non-technical issues – organizational structure, lines of authority, and – most importantly – human relations.

"Digital Disaster Recovery and Resources in the Wake of Superstorm Sandy: A Case Study" (Thomas F.R. Clareson) is the final chapter in the book. In addition to providing an interesting window into the activities of several institutions that were in the line of this destructive 2012 hurricane, it underscores the importance of collaboration and partnership in disaster scenarios.

Getting Started

The book is capped off by two helpful appendices that will be of interest to readers who are ready to act on the advice and inspiration provided in the main text and set their institution's own plan into action. While the appendices are limited to communication planning, the "Resources" section that follows six of the seven main chapters supplements these helpful hands-on materials.

Overall, Mallery's compendium is a well-considered, practical, and manageable resource for the information professionals involved, or for those who should be involved, in developing or refining their organization's plans for technological disaster. That is all of us. **END**

Crista Bradley can be contacted at crista.bradley@uregina.ca. See her bio on page 47.







BRADLEY DIERS GRYSIUK JOHNSON SCOFIELD SITTON WERFEL

Conducting a Business and Systems Analysis to Protect Your ECM Investment Page 20

Mark Grysiuk, CRM, CIP, has been in information management for more than 12 years, working as a technical writer, documentation specialist, and records management practitioner in Toronto, Ontario, Canada. For the past eight years, he has provided leadership in building defensible disposition programs in both private and public sector organizations. Grysiuk can be contacted at *mgrysiuk@gmail.com.*

Benefiting from the NIST Cybersecurity Framework Page 25

Meg Scofield is a records management specialist in Washington, D.C. Her business, Two Coffee Cups Consulting, provides records and information management support for federal agencies, businesses, and nonprofits. She received master's degrees in writing from Johns Hopkins University and in library science from the University of Maryland. She can be contacted at *meg@twocoffeecups.com.*

What Organizations Must Know About the 'Right to be Forgotten' Page 30

Erik Werfel, J.D., IGP, CIPP-US, CISSP, CEDS, is a technologist who has been a member of the technical staff and management at Fragomen, Del Rey, Bernstein and Loewy for more than eight years. He previously was a developer at Bright Ideas Software and Lucent Technologies. A certified Information Governance Professional, Certified Information Privacy Professional-US, Certified Information Systems Security Professional, and Certified E-Discovery Specialist, he earned a juris doctor degree from the University of Pennsylvani Law School and a bachelor or arts degree in economics from Hampshire College. Werfel is a member of the New Jersey Bar. He can be contacted at *erik.werfel@gmail.com.*

In Search of an Effective RIM or IG Program Page 34

Fred V. Diers, CRM, FAI, has more than 40 years of records and information management experience with multi-national organizations. He has successfully implemented sustainable records management programs on a global scale for companies operating in more than 80 countries. A significant component involves developing business rules pertaining to information lifecycle, including indexing, metadata, and retention standards. Diers is a past president of ARMA International, an Emmett Leahy Award and a Britt Literary Award recipient, and a worldwide lecturer on information governance subjects. He can be contacted at *fdiers@msn.com.*

Seven Things Records Destruction Vendors Are Afraid to Tell You Page 38

Robert (Bob) Johnson is the chief executive officer of the National Association for Information Destruction (NAID), the non-profit secure destruction industry watchdog organization he founded in 1994. He speaks and writes internationally on a wide range of issues related to data protection legislation, policy and compliance issues, and vendor selection criteria. In addition, Johnson is frequently sought out by policy makers around the world for guidance on data protection issues. He welcomes comments and questions. He can be contacted at *rjohnson@naidonline.org.*

Analytics Is for Everyone Page 44

Judy Vasek Sitton, CRM, is an information governance analyst for Kinder Morgan in Houston, Texas. In more than 30 years in records and information management, she has designed, implemented, and managed records and information across multiple industries, as an employee and as a consultant. Sitton is co-author of *Managing Active Business Records* published by ARMA International in 2014, and she has written several articles for national publications. A past member of the Institute of Certified Records Managers Board of Regents, she also has served as an advisory board member of the DeVry University Health Information Technology program. Sitton can be contacted at *Judy_Sitton@kindermorgan.com.*

How to Prepare for Techmageddon Page 45

Crista Bradley is the university records and information management archivist at the University of Regina in Saskatchewan, Canada, where she oversees the organization's RIM program and the management of university records in archival custody. She holds a master of arts degree in history – archival studies from the University of Manitoba. Bradley has served on the board of ARMA Saskatchewan and various committees of the Association of Canadian Archivists and the Saskatchewan Council for Archives and Archivists. She can be contacted at *crista.bradley@uregina.ca.*

AD INDEX CONTACT INFORMATION

5	**Fujitsu** *fcpa.com*
IBC	**NAID** *http://directory.naidonline.org*
3	**Institute of Certified Records Managers** 518.694.5362 – *www.ICRM.org*
FC, BC	**Recall** *recall.com*
9	**OPEX Corporation** *www.opex.com/agility*
IFC, 19	**Next Level** *www.arma.org/nextlevel*

CommandIG™

The Recall Advantage

CommandIG™ transforms the way you govern documents, giving you complete control at every step and from any location. Practical, affordable and comprehensive, CommandIG™ automates governance over digital and paper content with enterprise-grade security.

Learn more at recall.com

recall™